Development of an Malicious Insider Composite Vulnerability Assessment Methodology

THESIS

William H. King, Gunnery Sergeant, USMC

AFIT/GIA/ENG/06-06

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIA/ENG/06-06

Development of an Malicious Insider Composite Vulnerability Assessment Methodology

THESIS

Presented to the Faculty
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
In Partial Fulfillment of the Requirements for the
Degree of Master of Science

William H. King, B.S.
Gunnery Sergeant, USMC

June 2006

AFIT/GIA/ENG/06-06

Development of an Malicious Insider Composite Vulnerability Assessment Methodology

William H. King, B.S.
Gunnery Sergeant, USMC

Approved:

/signed/ 31 May 2006

Robert F. Mills, Ph.D. (Chairman) date

/signed/ 31 May 2006

Dennis D. Strouble, Ph.D. (Member) date

/signed/ 31 May 2006

Michael R. Grimaila, Ph.D. (Member) date

AFIT/GIA/ENG/06-06

Abstract

Trusted employees pose a major threat to information systems. Despite advances in prevention, detection, and response techniques, the number of malicious insider incidents and their associated costs have yet to decline. There are very few vulnerability and impact models capable of providing information owners with the ability to comprehensively assess the effectiveness an organization's malicious insider mitigation strategies.

This research uses a multi-dimensional approach: content analysis, attack tree framework, and an intent driven taxonomy model are used to develop a malicious insider Decision Support System (DSS) tool. The tool's output provides an assessment of a malicious insider's composite vulnerability levels based upon aggregated vulnerability assessment and impact assessment levels.

The DSS tool's utility and applicability is demonstrated using a notional example. This research gives information owners data to more appropriately allocate scarce security resources.

Acknowledgements

First, I would like to thank my wife. I am indebted to her patience, continued support despite the trying times, late hours, and missed occasions. She continues to give meaning to my life and I am truly blessed for each day we have together.

Next, I would like to thank my advisor, Dr. Robert Mills, for his guidance and support with this research effort. I would also like to thank Second Lieutenant Kevin Morris for the valued input that he provided this thesis effort as well as Captain Christopher Augeri, who unselfishly took time out of his Ph.D. work to lend his advanced Microsoft Excel skills to assist in the development of the malicious insider decision support system presented in this work.

I would also like to convey my appreciation to former AFIT graduate, Marine Corps Master Sergeant Juan Lopez, for his sincere interest in my research, constant motivation, and the added insight that he provided this thesis.

Finally, I would like to thank my two beloved children. Seeing their smiling faces and enthusiasm upon my return home each day touched my heart and served as a constant reminder of how truly blessed I am.

William H. King

Table of Contents

List of Figures

Figure Page

List of Tables

List of Abbreviations

Abbreviation		Page
CIA	Central Intelligence Agency	1
MIs	Malicious Insider(s)	1
ITFDM	Insider Threat Functional Decomposition Model	3
DSS	Decision Support System	4
ARDA	Advanced Research and Development Activity	6
AOL	American Online	8
IP	Intellectual Property	8
CSI	Computer Security Institute	10
FBI	Federal Bureau of Investigation	10
IT	Information Technology	12
NIST	National Institute of Standards and Technology	15
FTP	File Transfer Protocol	15
CIA	Confidentiality, Integrity and Availability	17
HIPPA	Health Insurance Portability and Accountability Act	18
DOS	Denial of Service Attacks	18
PDR	Prevention, Detection and Response	18
SPM	Schematic Protection Model	20
VA	Vulnerability Assessments	23
NASA	National Aeronautics and Space Administration	23
NPR	NASA Procedural Requirement	24
DSS	Decision Support System	29
USB	Universal Serial Bus	32
MIVA	Malicious Insider Vulnerability Assessment	34
CIRT	Computer Incident Response Team	37
RRR	Rank Reciprocal Rule	38

Abbreviation		Page
MIPIA	Malicious Insider Potential Impact assessment	44
GUI	Graphical User Interface	53
MCT	Marine Combat Training	90
MOS	Military Occupational Speciality	90
DFAS	Defense Finance and Accounting Service	90

Development of an Malicious Insider Composite Vulnerability Assessment Methodology

I. Introduction

1.1 Motivation

Until recently, organizations allocated most of their network and computer security budgets to securing network perimeters from outside attacks [30]. Focusing the majority of resources on protecting from outside attacks left information systems vulnerable to threats originating from within.

While the ratio of malicious actions due to insider attacks compared to outsider attacks varies between studies, researchers agree that malicious insider attacks have become a more prevalent threat to information systems and their associated adverse impacts can no longer be ignored [3, 15, 16, 20, 21]. In fact, the number of successful insider attacks are believed to be much higher then research indicates because many organizations do not report them for a variety of reasons. The most common reasons for 2005 are shown in Figure 1.1 [16].

Monetary losses incurred as a result of successful insider attacks can cripple an organization. In one case a "trusted" employee wrote a logic bomb that deleted a critical application which cost the organization over $10 million dollars in losses and the subsequent layoff of 80 employees [7]. In another well known insider threat case, a Central Intelligence Agency (CIA) agent, Aldrich Ames, supplied Russian adversaries with sensitive information that cost fellow CIA operatives their lives [35]. Analysis of known Malicious Insiders (MIs) indicates that any organization using information systems is susceptible to insider threats [18, 22, 35].

The threat posed by MIs presents a tremendous problem to security personnel who must develop and implement new mitigation strategies to protect critical organizational data. Traditional prevention and detection methods have limited effect

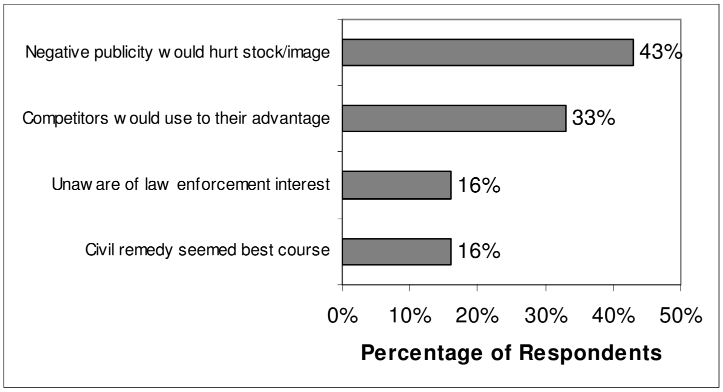


Figure 1.1: Non-Reporting Trends (639 respondents) [16]

against insider threats. While various methods have been used to prevent and detect insider threat activities, the frequency and costs associated with insider threat exploits have yet to decline [13–16]. Therefore, there remains a need for new methods to address the threat. However, simply investing money without an overall strategy to deal with problem can be both costly and ineffective. Therefore, an MI vulnerability assessment process that provides organizations a cost effective and reliable means for assessing and protecting against insider threats is needed.

1.2 Background

MIs are difficult to detect until after the damage has been incurred. Since most organizations rely on robust perimeters to protect from outside attacks [30]. Other contributing factors include: the level of trust given to employees, use of authorized access to conduct malicious actions, and the non-technical ease of exercising MI attacks [31].

Organizations often underestimate the potential threat from assuming typical system users do not posses the technical knowledge to carry out sophisticated attacks. The Internet offers a wide range of automated attack tools that provide sophisticated attacks to internal users having a low level of system access (Figure 1.2) [1].

Insider threat assessment research is examining increasingly effective methods to mitigate the MI. Anomaly detection, signature analysis, network monitoring sensors,

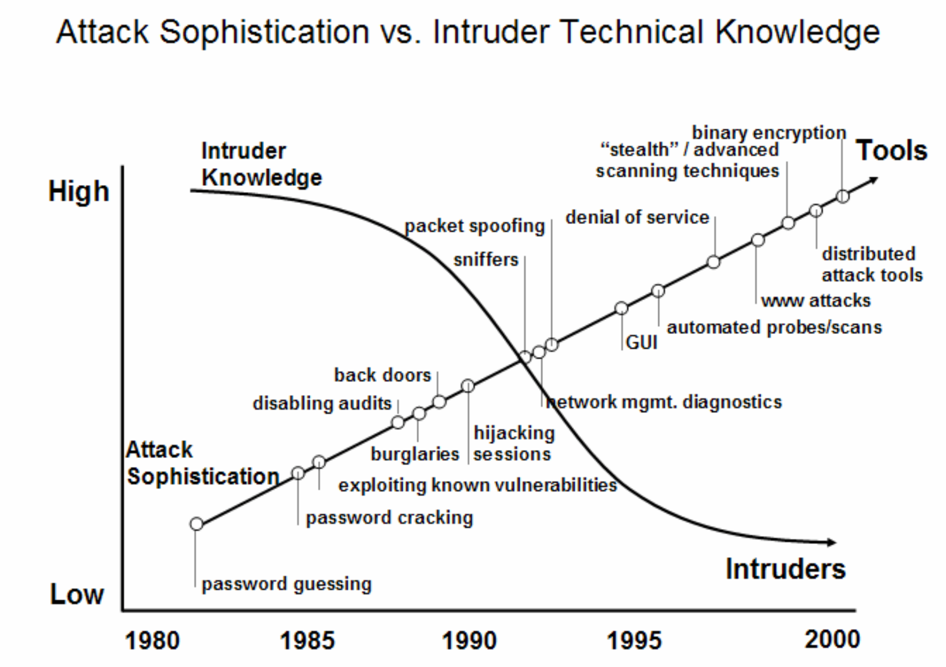


Figure 1.2: Historical Information Systems Attack Trends [1]

social network analysis, honey pots, and honey tokens are some of the primary MI areas of interest [3, 24, 30, 32, 33, 38].

While the research areas are significant contributions in the prevention and detection of potential insider threats, organizational management and security personnel also need to identify various MI actions that organizations must defend against. Furthermore, insider threat assessments that enable information owners to better understand their current MI vulnerability levels would also be of great benifit.

1.3 Purpose

This research provides information owners a methodology to determine an organization's malicious insider vulnerability levels. This, in turn provides a means of identifying and reducing risks to an acceptable level.

1.3.1 Objectives. The first objective of this research is to expand and improve an existing Insider Threat Functional Decomposition Model (ITFDM) [4]. The expanded ITFDM provides information owners with a standard method of identifying malicious actions.

The second objective of this research is to develop a process for conducting MI vulnerability assessments capable of providing information owners with qualitative and quantitative vulnerability metrics which measure an organization's current insider threat vulnerability level.

The final objective is to develop an MI impact assessment Decision Support System (DSS) that provides information owners with the means to assess the adverse effects of a successful exploit. The information owners can use this impact assessment results to evaluate and tailor MI mitigation strategies.

1.4 Scope

The application of the result of this research are intended for an organization's individual business units and not the organization as a whole. This scope allows for a sufficiently granular approach to vulnerability assessment by evaluating the effectiveness of MI mitigation strategies for each business unit.

Recent literature supports the notion that the majority of insider threat malicious activities did not require administrator access or a high degree of technical knowledge as shown in Figure 1.2. Therefore, this research focuses primarily on insider threats originating from users with typical system access [6]. Typical users can compromise critical company data by simply copying, e-mailing, or deleting a file from the server using the same access they use for their jobs, but with the intent of doing harm to their organization [7].

Typical users who unintentionally harm their organization's information system by accidently deleting a critical file or unknowingly compromising their password are another recognized category of insider threats, but are not addressed in this research. The terms insider threats and MI refer specifically to system users who intentionally exercise malicious actions within an organization's information system infrastructure.

1.5 Limitations

The insider threat taxonomy model developed in this research specifically addresses non-technical malicious insiders. MIs having technical networking skills or system administrator privileges introduce additional ways of exploiting system vulnerabilities. However, an additional insider threat action model that addresses technical users with system administrator privileges could be developed using an approach similar to that developed herein.

1.6 Intended Audience and Assumptions

This thesis assumes the reader is familiar with information systems and information technology terminology. Furthermore, this work assumes a basic level of understanding of commonly performed malicious actions.

Regardless of the robustness of MI mitigation strategies, every organization's information systems include some level of risk. However, the level of robustness of MI mitigation strategies do influence the risk levels.

During the course of this document, the terms insider threat and malicious insider (MI) are used interchangeably. Additional assumptions are discussed later in this document.

1.7 Document Overview

Chapter II presents an overview of current insider threat topics to include: characteristics, case studies, trends, risk assessment, information security as well as related research. Chapter III presents the methodologies used to achieve the objectives of this work. Chapter IV presents a notional example that demonstrates the practical application of an expanded insider threat decomposition model as well as MI vulnerability and impact assessment methodologies. Finally, Chapter V presents a summary of the research conclusions and recommended areas for future research.

II. Literature Review

This chapter presents insider threat: (1) background, (2) various detection challenges, (3) case studies, and (4) trends. The remainder of the chapter discusses related work and fundamental insider threat concepts.

2.1 Insider Threat Background

The proceedings of the 2005 Advanced Research and Development Activity (ARDA) challenge workshop, provides a comprehensive *insider threat* definition:

> An insider is anyone in an organization with approved access, privilege, or knowledge of information systems, information services, and missions. A malicious insider is one motivated to adversely impact an organization's mission through a range of actions that compromise information confidentiality, integrity, and/or availability [25].

2.1.1 Insider Threats Challenges. Insider threat detection is a very difficult problem. Organizations assume that their employees do not pose a significant threat to their information systems. One of the main contributing factors to this belief is the level of trust given to employees. It makes little sense to consider a new employee who was an"outsider" a week earlier, trust worthy. Their employment does not establish loyalty to the organization, nor does it mean that they would not perform malicious actions [7].

Another problem is the continued difficulty of of pairing a common profile to the threat. Law enforcement creates profiles for different types of crimes such as a kidnapper, bank robber, or murderer [30]. "However, with insider threats there is no demographic profile. People who have been caught vary in age, sex, social background, and education and cover the entire range of categories of people" [7].

The last difficulty is that insider can perform malicious actions much easier than outside attackers. Insider threats are more difficult to defend against due to their (1) authorized access to the system, (2) knowledge of processes and security practices, and (3) physical access to the system [37]. Systems security personnel can fairly easily detect outside attackers attempting to break into an organization's information system; however, it is far more challenging to distinguish whether a trusted employee who opens, modifies, copy's, or deletes a file is doing so in the performance of their duties or for malicious purposes.

2.1.2 Known Insider Threat Case Studies. The following six case studies illustrate the severe and sometimes devastating damage that has been inflicted across a wide range of organizations by MIs. Examination of known insider attacks provides valuable insight that can be used to develop more effective mitigation strategies.

Between 1986 to 1994, former CIA officer Aldrich Ames, received over $2.5 million dollars in exchange for providing classified CIA and FBI human source information to the Soviet Union [35]. Ames was sentenced to life in prison and is notoriously known for selling out fellow CIA agents, who subsequently were killed as a result of Ames' betrayal. It is of interest to note that despite Ames' spending beyond his means, his malicious activities went undetected for eight years. This serves as yet another example of an organization that did not understand its insider threat vulnerabilities and the potential impact of malicious activities.

In 1999, Thomas Varlotta, a disgruntled O'Hare aviation engineer was charged by a federal grand jury with damaging and stealing government property. He had misused his authorized system access to delete all known copies of the computer code that intended to fix errors in an application used to direct jetliners at the airport [18]. Varlotta drew suspicion when he quit the day after the code was deleted. A subsequent search of his home found the stolen code, which was encrypted and took six months to decipher.

In May 2000, Timothy Lloyd became the first American to be sentenced to prison under Federal Law for deleting critical organizational files [23]. Lloyd was motivated by revenge after his company demoted him. His organization, like many others, did not have adequate strategies in place to identify Lloyd's malicious actions. However, the prosecution was able to prove his guilt after forensic analysis of a hard drive found in his garage revealed time bomb code residing on it. His malicious actions cost his organization, Omega Engineering, an estimated $10 million dollars in damage.

In 2002, disgruntled employee, Roger Duronio, had with revenge as his motive when he planted a logic bomb on over 1,000 organizational computers. The resulting damage from the logic bomb cost his employer, PaineWebber, over $3 million dollars in monetary losses [7]. Duronio's revenge was fueled by what he felt were inadequate bonuses and a low salary.

In 2002, Melvyn Spillman was found guilty by a grand jury of using his computer network system privileges to redirect more than $4.9 million dollars from personal estate's liquidated assets into his personal banking accounting [7]. Spillman was motivated by greed, and like several other known MI's, his extravagant spending went unnoticed. In the three year period prior to being caught, Spillman sponsored a Formula One racing car despite having an annual salary of $33,000. Replacement parts alone for the racing car totaled over $250,000 in a single quarter [7].

In 2003, American Online (AOL) employee, Jason Smathers, used a fellow employee's access to obtain the screen names of over 92 million AOL customers. The employee subsequently sold the list to a third party for $100,000. In turn, the third party then sold the list yet again. The compromised customer list resulted in the customers on the list being spammed. The largest adverse impact to AOL was a tarnished reputation due to the organization's inability to protect sensitive customer information from their own employees. The incident also ended up in the Washington Post which had an adverse impact on potential customers [22].

While MI's do not share a common demographic profile, analysis of known insider threat cases have found some similarities exist between attackers. The following list provides the most commonly shared MI characteristics [36]:

- Minimal technical knowledge
- Attacks focused on intellectual property (IP)
- Driven by greed and revenge

- Displayed external indicators prior to their malicious actions (e.g., living outside of their means)
- Malicious actions typically resulted in greater monetary losses than would outside attacks

2.1.3 Insider Threat Studies. Prior studies provide a better understanding of insider threats, therefore findings from recent workshops, reports, and surveys are used to further understand the insider threat problem.

2.1.3.1 2005 Insider Threat Study. The United States Secret Service and the Carnegie Mellon Software Institute released their second annual Insider Threat report in May 2005. The purpose of the report was to document and better understand MI activities affecting information systems and data in critical infrastructure sectors [20]. The report examined forty-nine known insider threat cases that occurred between 1996 and 2002. This report found MIs were primarily motivated by revenge were more apt to perform acts of sabotage; whereas, MIs motivated by greed were more likely to exploit an organization's critical information. In 61% of the cases, insiders used unsophisticated methods of attack, which supports the notion that typical system users pose a serious threat to an organizations information systems [20].

The various methods of attack include automated scripts, toolkits, flooding, probing, escalation of privileges, scanning, and compromising another users account. In 56% of the cases remote account access was used.

Additionally, in 81% of the cases organizations experienced some financial loss as shown in Table 2.1. In 49% of the cases the average financial loss per internal malicious action was estimated at over $50,000. In 11% of the cases, losses totaled over $1 million per incident. These alarming figures further demonstrate the need of organizations to identify MI vulnerabilities and apply appropriate mitigation strategies. The figures

Table 2.1: Organizational Monetary Losses from Insider Threats [20]

Percentage of Organizations	Monetary Loss
2	Greater than $10,000,000
9	$1,000,000 - $5,000,000
7	$200,001 - $300,000
2	$100,001 - $200,000
11	$50,001 - $100,000
9	$20,001 - $50,000
42	$1 - $20,000

are based on data collected from 1996 to 2002. Losses today would likely be higher as organizations have increasingly invested in and rely upon information systems.

In many cases, insider attacks could have been prevented through the monitoring of employee behavior combined with a continued focus on reducing information systems vulnerabilities. The following lists the key findings from the Carnegie Mellon report [5]:

- Most insider attacks were triggered a result of negative work-related events
- 62% of the attacks were planned in advance
- 57% of the insider attacks exploited existing applications, processes, and/or procedure vulnerabilities
- 61% of the insider attacks did not require sophisticated attack tools
- Insider attacks caused financial losses 85% of the time and a negative impact to business operations 75% of the time

2.1.3.2 Survey Trends. Over the past 10 years, the Computer Security Institute (CSI) and the Federal Bureau of Investigations (FBI) have produced the longest known continuous computer crime security survey of its kind (*CSI/FBI Computer Crime and Security Survey*). The aim of the computer crime survey is to raise the level of security awareness as well as help determine the scope of computer crime in the United States [13].

The survey annually mails out anywhere from 3,500 to 5,000 surveys to computer security professionals working for corporations, financial institutions, government agencies, and universities within the United States. Yearly survey responses have ranged anywhere from 501 to 700 participants [13, 15, 16]. The 2005 CSI/FBI survey results indicated insiders are involved in nearly half of the known computer security incidents experienced by an organization (Table 2.2). The survey results also indicate similar rates of insider attack over the past four years. Thus, insider threats are not losing momentum.

Table 2.2: CSI/FBI Computer Security Incidents [16]

Number of insider threat incidents by % of respondents	**1-5**	**6-10**	**>10**	**Don't know**
2005	46	7	3	44
2004	52	6	8	34
2003	45	11	12	33
2002	42	13	9	35
2001	40	12	7	41
2000	38	16	9	37
1999	37	16	12	35

While the actual costs per incident as reported by insider threat research vary, the CSI/FBI survey has produced useful results that show the monetary loss incurred as a result of the most commonly performed malicious actions. Figure 2.1 illustrates the financial losses reported by organizations due to information systems security attacks in 2005. When compared to previous CSI/FBI computer security results, the figures indicate the increasing costs of virus-based attacks, theft of proprietary information, and unauthorized access. Collectively, these three categories accounted for over 80% of the reported financial loses in 2005. Each of the three categories can be accomplished using available means such as misusing authorized access and executing any number of malicious scripts available on the Internet. Typical system users are therefore in a prime position to carry out each of the these three increasing types of attacks using their granted access, knowledge of the system, and assumed level of trust [8].

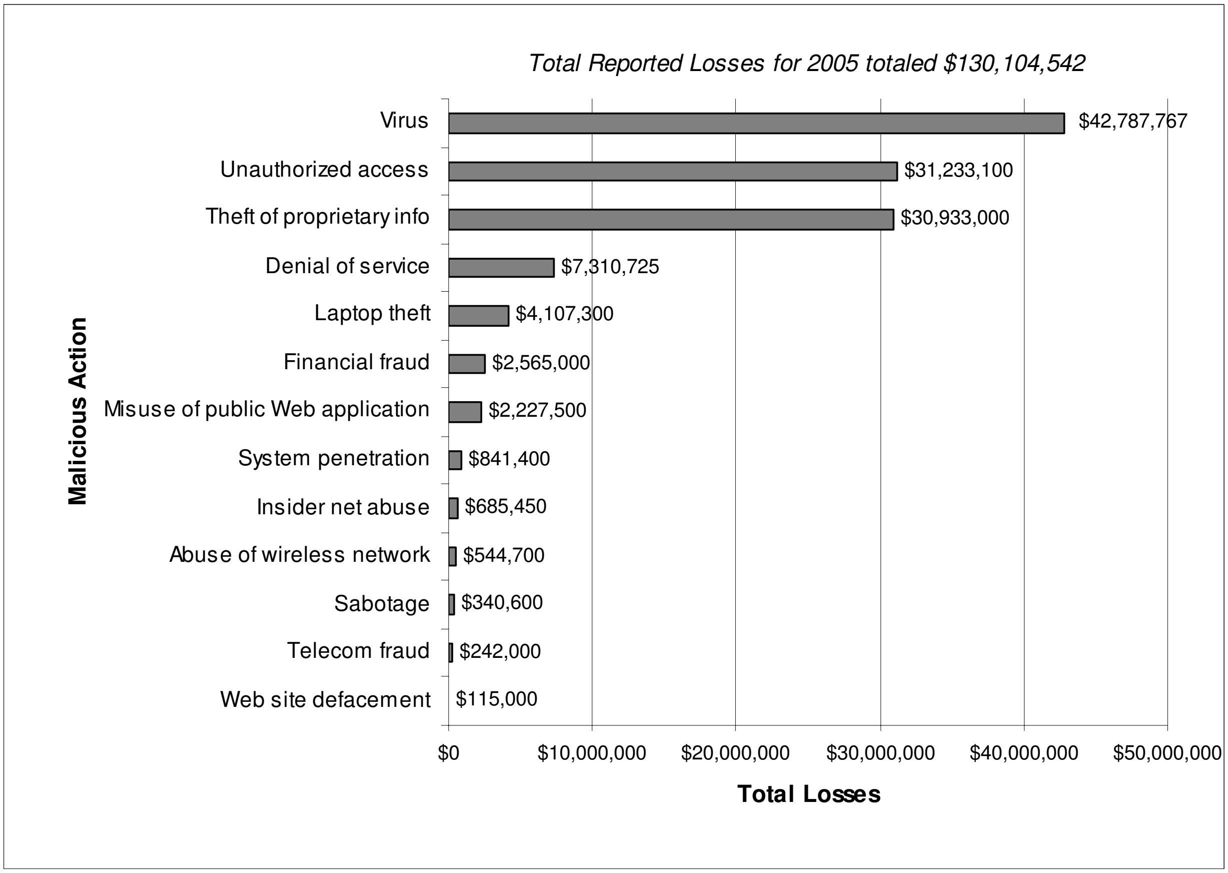


Figure 2.1: 2005 Reported Monetary Loss (N=690) [16]

Another notable survey finding is the percentage of the overall Information Technology (IT) budget that each organization allocates to its security budget. While the survey only recently started to include IT budget questions, there are some interesting conclusions that one can draw from the survey results. Figure 2.2 illustrates that 75% of the 2005 survey respondents spent between 1% and 10% of their total IT budget

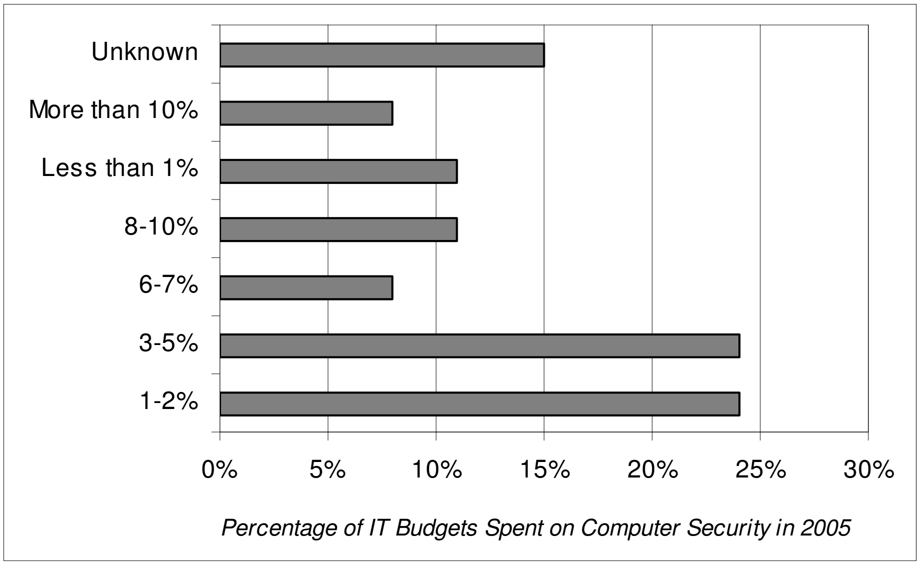


Figure 2.2: % of IT Budgets Spent on Security in 2005 (N=690) [16]

on system security, as opposed to 7% in 2004 [16]. This is a 3% increase from 2004, which indicates that organizations are allocating more of their IT budges to secure their network infrastructure. Another indicator that highlights an upward trend in IT spending is only 11% of the 2005 survey respondents reported spending less than 1% of the overall IT budget on system security, as opposed to the 16% reported in the 2004 survey.

One trend in the survey that has not been adequately addressed is the average cost of a successful insider threat incident. Many security professionals participating in the survey did not to disclose how much financial loss was incurred by their organizations as a result of MI activities. For those who did provide results, there is no means by which to verify the numbers because the survey is anonymous. For example, in 2002 the CSI/FBI survey results estimated the average financial loss per insider threat incident at approximately $2 million. In the 2003 survey, this number increased to over $2.7 million per incident and in 2004 that number fell to $526,000 per incident. The 2005 survey results reports a $203,000 loss per incident [13–16]. The figures are often guesses at best that vary depending on how each respondent measures lost revenues. While a disparity exists in the reported financial losses, even the smallest reported figure of $203,000 per incident indicates that MI actions are costly to an organization. This is especially true considering that insider threats comprise 46% of known computer system attacks [16].

2.1.4 Background summary. Some key concepts discussed in this background summary include:

- Malicious insider actions can and do occur in any organization
- The majority of malicious actions use non-technical means
- Insider threats are commonly motivated by greed or revenge
- Insider attacks are generally more costly than attacks originating from the outside
- Insider threat statistics can be misleading, because many are not reported
- Observable action models may provide a potential means in identifying and mitigating insider threats

2.2 Risk Assessment

Risk Assessment is, "The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact" [11]. A risk assessment can be accomplished either quantitatively, qualitatively or via a combination of the two. A threat assessment is a process that organizations can use to prioritize and determine what critical data needs to be protected.

2.3 Definitions

Having a general understanding of the overall risk assessment process provides a top-level view that can be used to develop a more effective MI vulnerability and impact assessment process model. While there are several variations, risk can be quantified as [7]:

$$Risk = \frac{threat * vulnerabilities * probability * impact}{.} countermeasures \tag{2.1}$$

Risk is defined by The National Institute of Standards and Technology (NIST) as “The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur” [11]. Assessing risks to critical data enable an organization to identify and reduce those risks to an acceptable level.

Threat is defined as, “The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability” [11]. Possible MI dangers attributed to information systems include violations of one or more protection states (unauthorized alteration, distribution, snooping and elevation) [2]. For example, the potential for an authorized user to perform unauthorized malicious activities is a threat.

Vulnerability is “A flaw or weakness in system security procedures, design, implementation, or internal controls that could be performed (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy” [11]. The effectiveness of threat mitigation strategies have a direct impact on information systems vulnerability levels. For example, an organization with inadequate File Transfer Protocal (FTP) vulnerability mitigation strategies are susceptible to MIs distributing proprietary information to unauthorized entities.

Probability is “... the likelihood that a potential vulnerability could be performed by a given threat-source” [11]. Probability is a difficult component of the risk formula to determine because it involves human factors. There is no way of being certain which employee will become an insider threat.

Impact is "... the adverse impact resulting from a successful threat exercise of a vulnerability (e.g.,, loss of public confidence, loss of credibility, damage to an organizations interest)" [11]. Impact levels can not be typically reduced without decreasing an information system's capabilities. The value of an organization's critical data has a direct bearing on adverse impact levels resulting from MI activities.

Countermeasure is "... the deployment of multiple defense mechanisms between the adversary and the target. To reduce the likelihood or affordability of successful attacks, each mechanism should present unique obstacles and include both protection and detection measures [10]. Implementing configuration management changes to prevent users from accessing external FTP sites is an example.

Information Owners are " System users who are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and the data they own" [11].

2.3.1 Risk Mitigation Options. The key components of a risk assessment model are threats and vulnerabilities. In the absence of any threat, there is no need to continue with the risk assessment process because the vulnerability cannot be exploited. However, threats inherently exist for critical data residing within information systems. This makes vulnerability the true key to the risk assessment process. After conducting a risk assessment, information owners may use the results to select one of six commonly used mitigation strategies [11]:

1. *Risk Assumption*: "To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level."
2. *Risk Avoidance*: "To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)."
3. *Risk Transference*: "To transfer the risk by using other options to compensate for the loss, such as purchasing insurance."

4. *Risk Limitation*: "To limit the risk by implementing controls that minimize the adverse impact of a threats exercising a vulnerability (e.g., use of supporting, preventive, detective controls)."
5. *Risk Planning*: "To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls."
6. *Research and Development*: "Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability."

Once MI vulnerabilities have been assessed, knowledge of the potential impacts will aid information owners in determining which risk mitigation strategy is most appropriate.

2.4 Information Systems Security

The following section discusses fundamental concepts that are an integral part of this research. To protect critical data, information owners need a method to determine and implement mitigation strategies that provide an acceptable level of risk.

2.4.1 Critical Data. Not all electronic data require the same level of protection. While various types of data reside on information systems, some data is considered more important and therefore requires added protection (e.g., mission essential data, data required by law to protect, and classified data).

Since organizations have a limited computer security budget, it is prudent for an organization to focus on identifying and protecting data according to it's assessed value [15,16]. Monetary worth, future benefit to the company, competitive advantage, as well as security classifications are various metrics that determine what data is most critical to an organization [11].

2.4.2 Security Objectives. MI actions adversely impact one or more of the three common security objectives: Confidentiality, Integrity, and Availability (CIA)

[11]. Assessing the adverse impact to each of the three security objectives allows information owners to more precisely determine the potential impact of MI actions.

Confidentiality is "... the protection of information from unauthorized disclosure" [11]. Critical information that an organization typically keep confidential include trade secrets, proprietary data, classified data, and data protected due to legal requirements (e.g., Health Insurance Portability and Accountability Act of 1996 (HIPPA), and Sarbanes-Oxley Act). If this information were to fall into the wrong hands it could have an adverse effect to an organization. For example, a programmer that uses their authorized access to copy proprietary software code and subsequently sells the code to a competitor breaches the confidentiality security objective and gives the competitor an unfair competitive advantage.

A loss of *integrity* is "... unauthorized changes made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions" [11]. The unauthorized modifications of critical data could prove detrimental to an organization. For an example, MI activities that compromise integrity could result in loss of life or poor decisions that could ruin a business.

A loss of *availability* is "The unavailability of an information system to its end users" [11]. Various methods to compromise data availability include denial of service (DOS), deleting critical files, or physically sabotaging a backup power supply. A loss of system information availability may result in a loss of productive time, thus potentially preventing system users accomplishing the organization's mission.

2.4.3 Information Security Elements. The three information security elements include Prevention, Detection, and Response (PDR). Assessing each of the PDR element's security levels provides information owners a method of measuring the effectiveness of an organizations MI mitigation strategies.

Prevention includes security controls that prevent insider threats from successfully exercising their methods (actions) of attack. Various preventive measures include authentication, authorization, nonrepudiation, encryption, and access controls [11].

Detection includes security controls that identify possible malicious activity and warn network/computer security personnel. Various detection measures include auditing intrusion detection systems [11].

Response includes security measures that mitigate the impact of malicious attacks to include: response and recovery plans, pre-established response teams, and environmental security (e.g., smoke alarms and sprinkler systems) [11].

Information security PDR levels are determined by the effectiveness of mitigation strategies that to protect data critical. Preventive security measures typically cost more to implement than detection measures. The robustness of the preventive measures depend on the value information owners place on their critical data [6]. For example, the FBI would likely have more robust and costly preventive measures to protect their most critical data than would a public library. In the case of a public library, MI detection measures that are less costly than preventive measures would likely be appropriate.

2.5 Related Work

This research effort combines prior taxonomies and vulnerability assessment processes in order to develop a more comprehensive MI composite vulnerability process. This section discusses various vulnerability and impact assessment methodologies.

Before determining insider threat countermeasures, it is first necessary to identify the threats and understand the MI's intentions and their associated actions. Cyber Observable and Attack Models [3] as well as Butts's Insider Threat Functional Decomposition Model (ITFDM) [4] describe approaches for identifying and classifying the more prevalent MI actions.

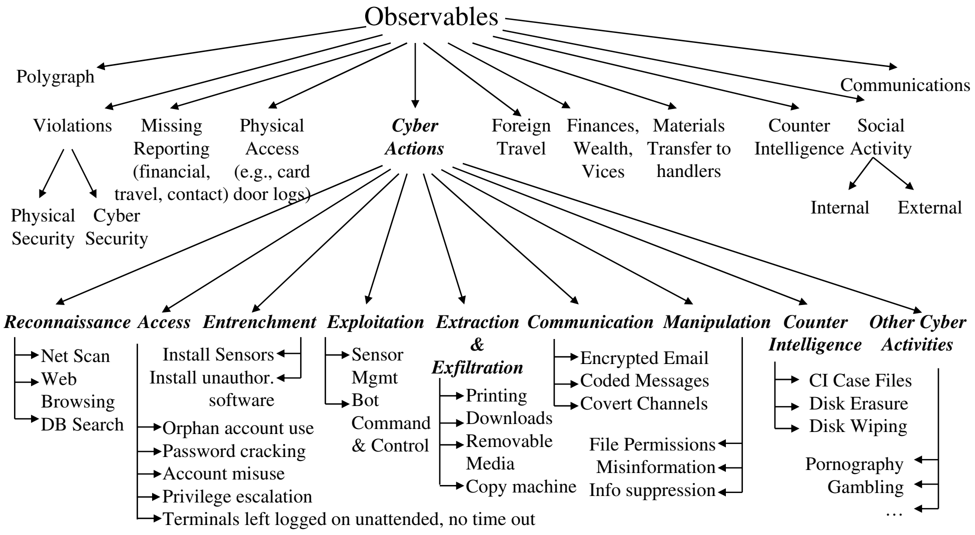


Figure 2.3: Cyber Observables Taxonomy [25]

2.5.1 Cyber Observable Taxonomy Model. The insider threat workshop conducted at the 2004 RAND conference produced two notable insider threat taxonomy models [3]. The Cyber Observables taxonomy model lists numerous *observable* malicious insider threat behaviors (i.e., actions) [3]. Figure 2.3 is the Cyber Observables taxonomy model. The model identifies and classifies methods used to carry out malicious activities. The Cyber Observables taxonomy model is one of the first known frameworks that identifies insider threat methods used to exploit vulnerabilities.

2.5.2 Attack Taxonomy Model. The Attack Taxonomy Model is based upon the analysis of known insider threat case studies which identified 33 methods (i.e., actions) to exploit information system vulnerabilities.

The Cyber Observable and Attack Tree Taxonomy models identified various malicious actions performed by MI's. ITFDM systematically incorporates and categorizes malicious actions identified by various sources (e.g., Cyber Observables and Attack Tree Taxonomy models), into a single framework using the Schematic Protection Model (SPM), attack trees, and functional decomposition. The ITFDM is a formalized model capable of categorizing unauthorized insider actions [4].

The protection state of a system is determined by the privileges possessed to the subjects (e.g., authorized users) [28]. ITFDM assumes that every potential user action results in an observable event in one or more of the following four exploits [4]:

1. *Alteration.* Alteration is the unauthorized modification of the information on an information system. Installing a key logger on a computer or deleting a critical database are two examples. In both cases the MI altered an object from one state to another in an unauthorized manner.
2. *Distribution.* Distribution is the unauthorized transfer of information from one entity to another. An example is a user who misuses authorized system privileges to transfer (e.g., electronic mail) a sensitive file to an unauthorized user.
3. *Snooping.* Snooping involves accessing or viewing information without a need-to-know. An example is a user who misuses authorized system privileges to access and/or view files without a valid need-to-known (e.g., employee salaries).
4. *Elevation.* Elevation occurs when a user escalates their system privileges beyond what was authorized. For instance, when a user gains unauthorized privileged access to a system which exceeds those previously assigned.

2.5.2.1 Attack Trees.

Attack trees provide the ITFDM with a hierarchical way to describe the security of a system [29]. The attack tree approach also allows the ITFDM to decompose the malicious insider threat. Figure 2.4 illustrates an example of the attack tree approach that categorizes the four actions of the MI.

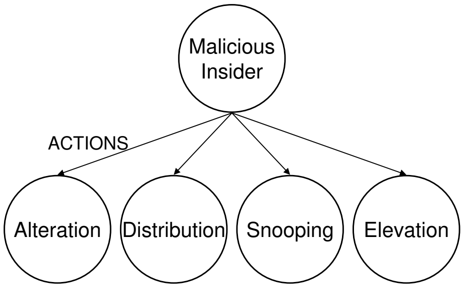


Figure 2.4: Root and 1st Tier ITFDM Action Leaf Nodes [4]

A key notion of attack trees is if a leaf node can be compromised, then the corresponding parent node is vulnerable as well. Figure 2.5 is an example of the parent to leaf node relationship using a combination safe (i.e., vulnerability) as the parent node. The leaf nodes describes various ways to compromise the safe (i.e., parent). If any of the methods can be successfully exploited, then the parent node is vulnerable. Attack trees allow information owners to identify the compromise vectors of the parent node.

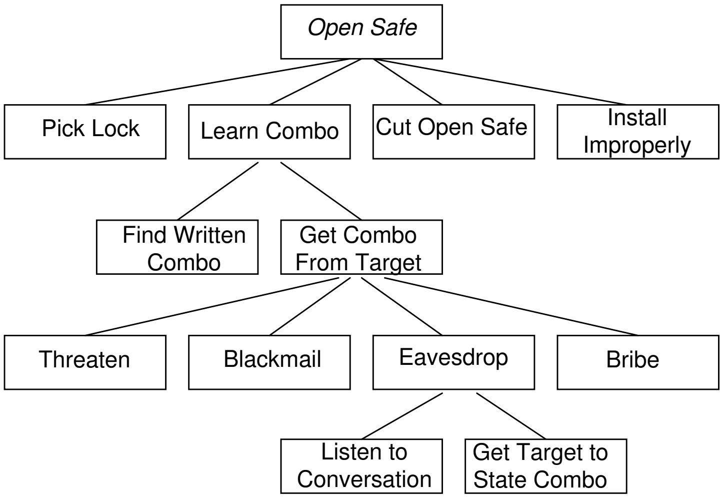


Figure 2.5: Attack Tree Scenario Example [29]

2.5.2.2 Functional Decomposition. ITFDM systematically decomposes MI actions. The resulting hierarchical structure provides a visual mapping of the precise path taken by the MI [4]. Figure 2.6 shows various paths a malicious insider could take to perform an unauthorized distribution. The greatest benefit of ITFDM is that it provides a comprehensive representation of possible insider threat actions.

The multidisciplinary approach of the ITFDM is more conducive for further development of an MI taxonomy. This strategy would enable an organization to precisely analyze and assess insider threat activities.

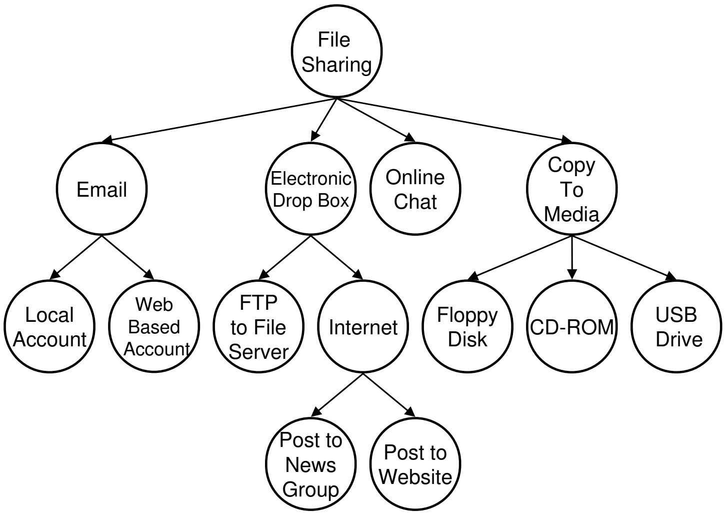


Figure 2.6: Distribution Example: File Sharing [4]

2.5.3 Vulnerability Assessment. Vulnerability assessments (VA) are a way to evaluate MI vulnerability levels and mitigation strategies [11,19,27]. For example, if a VA determines current mitigation strategies do not account for an MI installing a root kit on an information system, additional mitigation strategies should be considered. After implementing further mitigation strategies, another VA could be performed to determine if the vulnerability to the root kits has been reduced to an acceptable level of risk. The following section discusses three VA methodologies to include: the Los Alamos 12-step VA framework, The National Aeronautics and Space Administration (NASA) Vulnerability Assessment process, and the NIST Vulnerability Assessment Guide 800-30.

2.5.3.1 Los Alamos 12-Step Vulnerability Assessment Framework. The 12-step VA framework uses a penetration testing strategy to identify, mitigate, and re-assess methods of exercising malicious actions [19]. The primary assumption of the framework relies upon the creativeness of individuals within a group to collaborate and identify possible methods that an MI could use to carry out malicious actions. Consider the example of an open window [19]. A risk management process would ignore the open window if a specific vulnerability wasn't recognized; otherwise, the window would be closed and locked. The 12-step VA methodology would view the open window as an opportunity for MI mischief [19]. While brainstorming, participants think like a "bad guy" and consider the worst case scenarios for every situation. Below are the 12 steps identified in the VA model [19]:

1. Fully understand the device, system, or program and how it is really used
2. Play with it
3. Brainstorm
4. Play with it again
5. Edit and prioritize potential attacks
6. Partially develop some attacks
7. Determine feasibility of the attacks
8. Devise countermeasures
9. Perfect attacks
10. Demonstrate attacks
11. Rigorously test attacks
12. Rigorously test countermeasures

The application of the this framework is questionable due to vagueness of the 12-step process. The framework relies upon the creative ability of brainstorming teams to identify the actions an MI could use as opposed to using MI historical data to identify potential MI actions. Another limitation is individual members of the brainstorming team may conform to the general viewpoint of the group (i.e., group think). Because of this phenomenon, the group would be in jeopardy of not identifying an appropriate collection of MI actions. This VA process is also costly to an organization considering the number of man-hours required to perform each step. The model depends upon the diversity of the teams, and the experience of each member. Some organizations may have the ability to put together a very diverse and experienced team, while others may not.

2.5.3.2 NASA Vulnerability Assessment Process. The NASA Procedural Requirement (NPR) 1620.2 provides in-house compliance procedures for conducting physical vulnerability risk assessments [27]. The NPR outlines a systematic

Table 2.3: Asset Value Weighting [27]

Asset Characteristics	Value Weighting Factor
Fewer than 20 systems (i.e., computers) are in the facility. Does not include super-computing system(s) or systems processing sensitive or classified information.	1
Fewer than 20 systems (i.e., computers) are in the facility. Includes local area Networks and/or super- computing system(s) or systems processing sensitive or classified information.	2
More than 20 but less than 50 systems (i.e., computers) are in the facility. Does not include super-computing system(s) or systems processing sensitive or classified information.	3
More than 20 but less than 50 systems (i.e., computers) are in the facility. Includes local area networks and/or super-computing system(s) or systems processing sensitive or classified information.	4
50 or more systems (i.e., computers) are in the facility or the facility houses super-computing system(s) that is/are processing sensitive or classified information.	5

physical security assessment methodology that are applicable and beneficial in the development of an MI vulnerability assessment process.

NASA's physical security methodology identified and prioritizes critical assets that fall into one of two categorizes: human or facility. NASA's reasoning is based on lessons learned from terrorist attacks over the past 15 years. History has shown that terrorists typically attack facilities that contain a high concentration of people in one location. The NPR consists of 18 definition tables with value weights assigned that are applied according to the given asset and range from experimental animals to the relative value of arms, ammunitions, and explosives. Table 2.3 was developed by NASA to assess and prioritize information system related assets.

NASA's methodology also defines three weighting factors for the vulnerability level of critical assets. Each factor is weighted according to its classification mapping in the corresponding definition tables. The three vulnerability factors include asset accessibility, compliance with security requirements, and other physical deterrence measures [27]. The complete process is recorded on the NASA Physical Security Vulnerability Risk Analysis Worksheet (NASA form 1713 - provided in Appendix A).

This methodology demonstrates the usefulness of (1) determining the value of critical assets by using weighting factors and (2) using robust definition tables in the VA process. However, this methodology does not consider the potential impacts to an organization resulting from exploited vulnerabilities. Understanding the potential impact would aid information owners in determining if the vulnerability has been reduced to an acceptable level of risk.

2.5.3.3 NIST Vulnerability Assessment Guide.

NIST's Risk Management Guide for Information Technology Systems (Special Publication 800-30) provides a methodology for conducting vulnerability and impact assessments. The guides uses a nine-step approach in three phases: identification, counter-measure evaluation, and mitigation strategy implementation (flowchart diagram provided in Appendix B).

The NIST methodology is useful because it: (1) applies a systemic and linear approach to the entire process, (2) qualitatively evaluates vulnerabilities, and (3) provides a qualitative evaluation of the potential impact to the organization.

However, the NIST methodology: (1) uses broadly defined vulnerability tables and (2) does not pair the vulnerability and impact assessment results to derive an aggregated evaluation of the risk to an organization.

The NIST approach also includes an impact assessment component that is not found in the 12-step or the NASA NPR 1620.

2.5.4 NIST Impact Assessment.

According the NIST guide, the first step in performing a risk assessment is to gather specific information on three key organizational elements: (1) mission essential processes, (2) asset values, and (3) prioritized lists of critical assets. The guide recommends two methods for collecting the informa-

Table 2.4: NIST Impact Definition Table [11]

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede organizations mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

tion: (1) analyzing existing documentation and (2) determining the level of protection required for each asset to maintain it's desired state of Confidentiality, Integrity, and Availability (CIA) [11].

The NIST impact assessment methodology assigns various qualitative (e.g., high, medium, low) impact levels based on the degradation severity of the CIA security objectives. Table 2.4 provides the impact definitions for each qualitative level's magnitude of impact.

The NIST methodology is the only reviewed methodology to assess the potential impact to an organization resulting from MI activity.

The NIST impact assessment limitations include: undeveloped definition tables, does not provide an aggregate level of risk (i.e., vulnerability and impact assessments), and equal distribution of CIA security objective impact levels. For instance, if only one category (i.e., confidentiality) has a high impact as a result of an MI action, the other two CIA security objective components are arbitrary assigned high impact levels as well. By overstating impact levels, information owners will allocate resources in a manner inconsistent with the level of residual risk.

2.6 Chapter Summary

This chapter reviewed previous research in threat taxonomies as well as three risk assessment methodologies. The MI taxonomies, risk assessment methodology, and impact assessment have been integrated in this research effort to achieve a richer framework of MI activities. This framework provided the foundation for the development of a vulnerability assessment process that an information owner can use to more precisely assess the composite risk to information and information systems.

III. Methodology

This chapter outlines the methodology used to further develop an existing Insider Threat Functional Decomposition Model (ITFDM), develop formal MI vulnerability and impact assessment processes, and create a Decision Support System (DSS) proof-of-concept tool capable of assessing insider threat composite vulnerability levels.

3.1 Problem Definition

This research addresses the two topics areas of MI vulnerability and impact assessment. There are few vulnerability and impact models that are capable of providing information owners the capability to comprehensively assess the effectiveness of their MI mitigation strategies.

3.1.1 Research Goals. The three research goals include: (1) further decomposition of an existing ITFDM; (2) development of MI-specific vulnerability and impact assessment models; and (3) development of a DSS tool that can assess the effectiveness of an organizations MI mitigation strategies.

3.1.2 Expected Outcomes. It is expected that once the proof-of-concept tool is developed, information owners will be able to more comprehensively evaluate the effectiveness of an organization's MI mitigation strategies. In turn, this should allow the information owners to allocate scarce security resources more effectively when mitigating malicious insider threat risks.

3.1.3 Methods. First, the attack tree method was used to further decompose the ITFDM. The added level of granularity was grounded on MI intentions and associated actions.

Secondly, a content analysis of existing insider threat research was performed to collect a variety of insider threat intentions and associated actions.

Thirdly, this research used a multi-dimensional approach to developing MI-specific vulnerability and impact assessment models. A secondary benefit of this approach is that it allows the development of a composite vulnerability risk score which provides a more comprehensive assessment of overall risk. The multi-dimensional approach was achieved by integrating the PDR (i.e., prevention, detection, and response) and CIA (confidentiality, integrity, and availability) elements in the vulnerability assessment process. In addition, the evaluation criteria expanded the qualitative evaluation criteria from three to four categories and added a quantitative dimension for further ease of evaluating risk.

Lastly, this research developed a DSS proof-of-concept tool using Microsoft 2003 Excel Spreadsheet software.

3.2 Taxonomy of the Insider Threat

ITFDM provides a novel insider threat taxonomy framework. This research builds upon the model through further decomposition of the insider threat. The extended ITFDM is grounded on MI intentions and their associated actions.

3.2.1 Approach. Analysis of existing research will determine the more prevalent malicious actions performed by insider threats. A method that adds further granularity to the existing insider threat taxonomy model is also developed. Once expanded, the extended taxonomy model provides information owners with an improved framework that presents common MI actions. The extended model serves as a foundation for the MI vulnerability assessment and impact processes developed later in this research.

3.2.1.1 Content Analysis. Analysis of existing insider threat research, case studies, and surveys provided a way to determine the more prevalent malicious actions performed by insider threats. The methodology includes analysis of a number of sources to determine commonalties in insider threat actions that exist in the sources. The key component of this methodology relies on the analysis of a number of recent sources to create a more comprehensive list of various malicious actions performed from within an organization.

Moore's law states that as processing power doubles every 18 months, information systems capabilities also increase [9]. Subsequently, Moore's law implies that new insider threat actions will continue to emerge and become easier to accomplish. For example, "thumb drives" did not exist five years ago and therefore did not pose a security risk. If the content analysis process accomplished today did not include recent MI research, case studies, or survey material, thumb drives may have not have been identified as potential method for exercising malicious actions. Primarily for this reason, it is necessary to include recent research sources into the content analysis process when updating the taxonomy model.

While numerous documents were examined, this research focused primarily on the eight separate sources [3, 7, 11, 13–16, 20]. Each source were found to be both recent and inclusive in terms of addressing malicious actions performed by MIs. The content analysis methodology used in this research considers malicious actions as a common occurrence when identified in two or more of the sources and where then incorporated into the extended ITFDM.

3.2.1.2 Extending the ITFDM. The MI actions identified in the content analysis phase were categorized according to various possible MI *intentions*. The result is a more comprehensive intent-based ITFDM that lists each applicable action under the various intentions.

Prior to determining insider threat intentions, the more prevalent MI actions identified (Section 3.2.1.1) are categorized into the four states in the ITFDM (for convenience, Figure 3.1 is a repeat of an earlier figure from Chapter II). Next, each malicious action is analyzed and re-classified to determine the MI's primary intent. After the intention of each action has been identified, actions sharing similar MI intentions are grouped together.

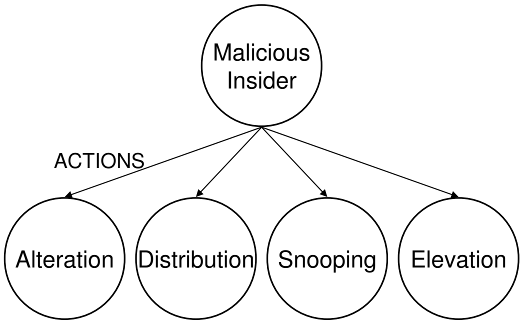


Figure 3.1: Root and 1st Tier ITFDM Action Leaf Nodes [4]

Figure 3.2 is the sixteen MI's intentions identified in this research. Figures C.1-C.4, map each malicious action to the MI's applicable intention (located in Appendix C).

3.2.2 Evaluation. The intent-based ITFDM provides clarity to the model while also enhancing the utility of the model. Emerging technologies introduce new vulnerabilities in information systems which leads to new ways for MIs to exploit information systems. Therefore, to preserve the utility of the modified ITFDM the model should be updated on an annual basis to ensure it contains current vulnerabilities.

While the methods to exploit vulnerabilities vary with time, MI intentions generally remain constant. For example, the added capabilities made possible through the introduction of Universal Serial Bus (USB) ports presented MIs with new methods to exploit information systems. MIs can use thumb drive technology to copy an organization's critical data for malicious purposes. Determining where to place the MI thumb drive exploit action in the now *intent-based model* can be performed by mapping the malicious action to the applicable malicious intention. In this case, the primary malicious intention that is most applicable to the malicious use of thumb drive technology is unauthorized file distribution (located in Appendix C - Figure C.2).

Another added benefit of classifying malicious insider actions based upon their primary intention is that information owners now have a means of focusing on their

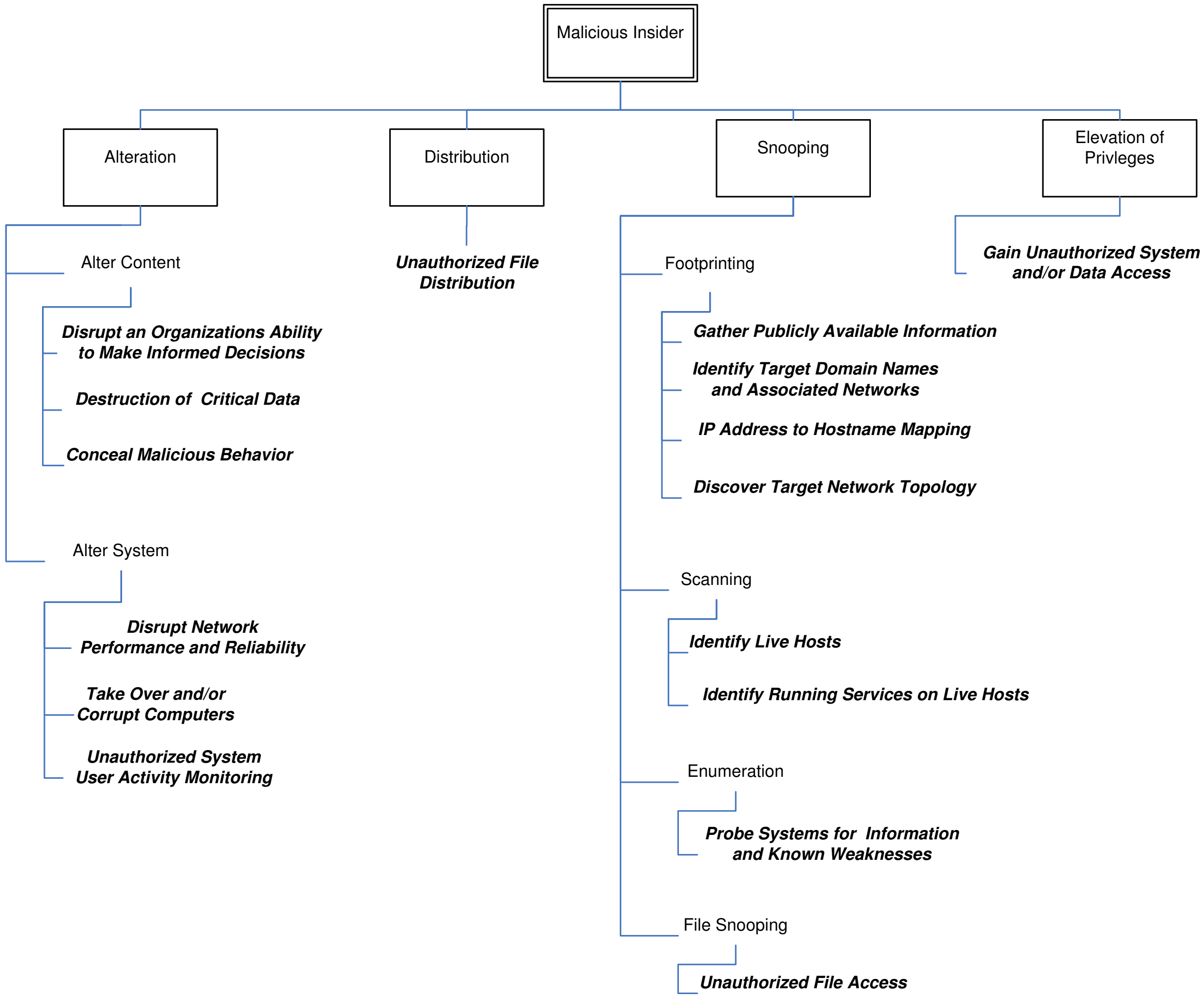

Malicious Insider
Alteration
Distribution
Snooping
Elevation of Privleges
Alter Content
Disrupt an Organizations Ability to Make Informed Decisions
Destruction of Critical Data
Conceal Malicious Behavior
Alter System
Disrupt Network Performance and Reliability
Take Over and/or Corrupt Computers
Unauthorized System User Activity Monitoring
Unauthorized File Distribution
Footprinting
Gather Publicly Available Information
Identify Target Domain Names and Associated Networks
IP Address to Hostname Mapping
Discover Target Network Topology
Scanning
Identify Live Hosts
Identify Running Services on Live Hosts
Enumeration
Probe Systems for Information and Known Weaknesses
File Snooping
Unauthorized File Access
Gain Unauthorized System and/or Data Access

Figure 3.2: ITFDM Malicious Intentions.

primary areas of concern and associated actions. Depending on an organization's mission and critical data, some MI intentions and associated actions are more applicable than others. For example, a university library may not be as concerned as a military intelligence center about the MI intention of *disrupting the organization's ability to make informed decisions*; however, the library is likely to be more concerned about the malicious intent of *disrupting network performance and reliability* (located in Appendix C - Figure C.1). The improved ITFDM now allows organizations to focus on specific MI intentions of concern and associated actions commonly used to exploit the intentions.

3.3 Vulnerability Assessment Process

Existing vulnerability models cannot provide information owners with an effective methodology for measuring their organization's MI vulnerability. This research uses a novel approach to develop an MI-specific vulnerability assessment process that effectively measures insider threat mitigation strategies. This process also provides greater granularity in the MI vulnerability assessment process then the NIST and NASA approaches [11, 27]. While other vulnerability assessment methodologies use a single definition table to classify vulnerabilities, this research uses three definition tables. This provides a more comprehensive assessment of the effectiveness of an organization's MI mitigation strategies than do other existing vulnerability assessment processes.

3.3.1 Approach. This research develops a Malicious Insider Vulnerability Assessment (MIVA) process that measures the effectiveness of information owner's MI mitigation strategies and determines existing subsequent MI mitigation strategies security levels. Once each PDR component is assessed, the combined security levels (i.e., vulnerability levels) are categorized into an overall security level.

The MIVA process correlates higher MI security levels to lower insider threat vulnerabilities levels; lower MI security levels correlates to higher insider threat vulnerabilities levels. Prior to developing steps that comprise the MIVA process, common security elements are defined. The common security elements (i.e., PDR) classifications in Figure 3.3 serves as the foundation for the MIVA process.

3.3.2 Common Security Element's Definition Tables. Individual PDR definition tables are critical elements to determining the MI security levels in the MIVA process. In each PDR component definition table, the key words that separate high, medium, and low in each definition are *italicized.* The various definitions in each table are carefully modified vulnerability assessment definition tables used in existing research to specifically apply to the MI and PDR security elements [27].

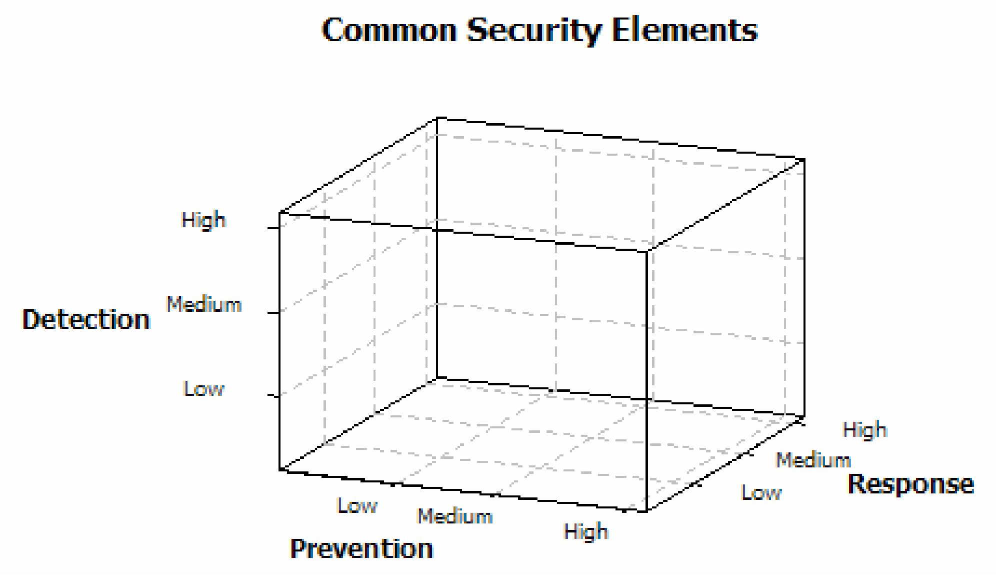


Figure 3.3: Security Elements Security Model.

3.3.2.1 Individual PDR Definition Tables. The first PDR definition table for prevention classifies security levels according to MI mitigation strategy's ability to prevent typical system users from exploiting information system vulnerabilities. Table 3.1 defines the three prevention classifications used in this research.

The second PDR component, detection, defines security levels according to MI mitigation strategy's ability to detect typical system users who attempt to exploit information system vulnerabilities. Table 3.2 defines the three detection levels.

The security levels for the last component in PDR, response, are classified according to MI mitigation strategy's ability to respond and recover from successfully performed MI actions. Table 3.3 defines the three response levels.

3.3.2.2 Aggregate PDR Security Level Definition Table. Table 3.4 combines the assessed security level results and arranges them from highest to lowest security level order from each of the PDR component tables (Tables 3.1-3.3). Again, the key words that separates the security levels in each definition are *italicized*.

Table 3.1: Prevention Security Level Definitions

Prevention Security Level	Definition
High	Prevention policies, procedures, and preventive controls make it *highly unlikely* for typical system users to exercise the malicious action. Data encryption is utilized.
Medium	Prevention policies, procedures and preventive controls make it *unlikely* for typical system users to exercise the malicious action. Group permissions and/or access control lists (ACLs) are utilized.
Low	Prevention policies, procedures, and preventive controls *do not prevent* typical system users from exercising the malicious action.

Table 3.2: Detection Security Level Definitions

Detection Security Level	Definition
High	Detection measures provide *near-real time to real-time* discovery and notification of the attempts by typical system users to exercise a particular action.
Medium	Detection policies, procedures, and detection controls *can likely identify* a typical system user who exercises a malicious action after the fact. Discovery after the fact prevents the user from carrying out further malicious actions and also serves as a deterrent to other potential MIs.
Low	Detection policies, procedures, and detection controls are *inadequate* to discover a given malicious action performed by an typical system user.

Table 3.3: Response Security Level Definitions

Response Security Level	Definition
High	Response measures have a *near-real time ability* to recover and defend critical data as well as collect and preserve evidence. This level of response ensures the least possible amount of financial harm and/or lost data. Response policies, procedures, and response mechanisms can include: • Established access to a primary and alternate Computer Incident Response Team (CIRT) • Forensic tools such as Encase Enterprize Edition that can provide the CIRT immediate online ability to respond, confirm, and contain malicious actions. Examples include: 1. Existing, tested, and continually updated data recovery and insider threat checklists 2. Extensive critical data recovery plans are in place and periodically tested
Medium	Response measures have a *delayed ability* to recover and defend critical data as well as collect and preserve evidence. Reasons for the delays may include: • Lack of CIRT availability • Ineffective forensic tools and/or inability to fully employ forensic tools • Infrequently tested data recovery and insider threat checklists
Low	Response measures have an *ineffective ability* to recover and defend critical data. There is also an inability to collect and preserve evidence, which can result in the greatest possible financial and data loss. Contingency checklists may exist but are ineffective and likely lack frequent and/or practical application testing.

3.3.2.3 Classification Levels. While each of the individual PDR component tables contain three classification levels (high, medium, and low), the aggregated PDR security level table adds two sub-classification levels within the high category (i.e., high and very high) to further distinguish between assessed PDR aggregated scoring. MI mitigation strategies assessed at higher security levels implies lower MI vulnerability levels and lower value-weighting, while lower assessed security levels implies lower MI vulnerability levels.

When one of the PDR components is assessed with a low security level, the combined PDR security level results in a high vulnerability classification. The vulnerability to the assessed MI action increases proportionally as the security levels of the other two PDR component levels decrease. Each decrease results in greater vulnerability. For example, PDR assessment scores of low, low, and low represent a greater vulnerability to MIs than PDR element scores of low, high, and high. The PDR security level table recognizes this and accounts for the potential differences in assessed security levels by taking the standard classification for high and subdividing it into two categories: very high and high vulnerability.

3.3.2.4 Vulnerability Level Value Weighting. The value weighting classification approach is a departure from methods used in other vulnerability assessment research. Existing vulnerability assessment methods commonly define three possible vulnerability levels and assign low levels a weighted value of 0.1, medium levels a weighted value of 0.5, and high levels a weighted value of 1.0. This classification level value-weighting approach adequately addresses the three possible vulnerability assessment outcomes (high, medium, low), but does not address the ten possible vulnerability assessment outcomes of the aggregated PDR security level definitions(Table 3.4).

This research uses a novel approach to assign discrete weighted values to quaternary individual PDR security levels using the Rank Reciprocal Rule (RRR). The RRR is a decision analysis tool that provides management with tangible values that are based on ordinal scales (e.g., classification levels). The RRR was found to be an appropriate tool, as the approach provides information owners with a more straightforward means of interpreting vulnerability levels.

RRR assigns quantitative ratio values relative to qualitative classifications [34]. It is capable of describing the weighted variations between classifications rather than assigning arbitrary values. Using this method, respondents rank attributes (i.e., category levels) can be arranged by importance from highest to lowest. Using the rank reciprocal rule formula (3.1), the ranks are transformed into normalized weighted values [34]

$$w_i = \frac{1/R_\iota}{\sum\limits_j 1/R_j}. \tag{3.1}$$

where w_i is the normalized weight of the ith attribute, R_i is the rank number, and the denominator is the sum of the inverses of all ranks.

Using the classifications of high, medium, and low, the following example demonstrates a practical application of the rank reciprocal rule [34].

$$w_\iota = w_H = \tfrac{1/1}{1/1+1/2+1/3} = \tfrac{1}{11/6} = 0.55$$

$$w_\iota = w_M = \tfrac{1/2}{1/1+1/2+1/3} = \tfrac{1/2}{11/6} = 0.27$$

$$w_\iota = w_L = \tfrac{1/3}{1/1+1/2+1/3} = \tfrac{1/3}{11/6} = 0.18$$

where w_H is the highest level attribute, w_M is the second highest level attribute, and w_L is the lowest level attribute.

The numerical values in Table 3.4 are the result of the application of the RRR to assign an overall quantitative value to each of the ten potential vulnerability assessment outcomes. The corresponding weighted vulnerability values increase as the vulnerability level increases (lower assessed PDR security levels). For example, a PDR assessment resulting in all high security levels has a lower combined vulnerability value than would a PDR assessment resulting in all low security levels. The higher the security level, the lower the vulnerability level; the lower the vulnerability level, the lower the corresponding weighted value. The RRR also accounts for vulnerabilities inherent to information systems. While small, even the lowest MI assessed vulnerability level (all high PDR security levels) still has a weighted value (0.03) indicating that some vulnerability exist. This is fitting as vulnerabilities are inherent to imperfect man-made information systems and there is no method by which vulnerabilities can be completely mitigated.

Table 3.4: Combined PDR Vulnerability Classifications Definitions with Corresponding Individual PDR Security Level Possibilities

Combined PDR Vulnerability Classification (with Associated Security Levels)	Definition
Very High Vulnerability Low-Low-Low (0.34) Low-Low-Medium (0.17)	Policies, procedures, and preventive controls *allow* typical system users to potentially carry out malicious actions. The vulnerability is unacceptable in varying degrees due to the ineffectiveness of policies, procedures, and preventive controls to prevent, defend, or respond to malicious insider actions.
High Vulnerability Low-Low-High (0.11) Low-Medium-Medium (0.09) Low-Medium-High (0.07) Low-High-High (0.06)	
Medium Vulnerability Medium-Medium-Medium (0.05) Medium-Medium-High (0.045) Medium-High-High (0.035)	Policies, procedures, and preventive controls make critical data exposure to potential insider threats *unlikely* in varying degrees. However, should an insider successfully carry out malicious actions detection of and response to the threat could occur after the fact.
Low Vulnerability High-High-High (0.03)	Policies, procedures, and preventive controls allow for a minimal critical data exposure risk level. It is *highly unlikely* that typical system users could successfully carry out malicious actions and if they did, near to real-time detection and response measures could identify the risk.

3.3.2.5 Evaluation. The PDR security level definitions offer a greater level of robustness than existing vulnerability assessment frameworks thus allowing for a more comprehensive insider threat vulnerability security posture. Another improvement is the development of vulnerability assessment that subdivide the high vulnerability classification outcomes into high and very high sub-levels. The corresponding weighted values also more accurately capture the variances between vulnerability assessments outcomes.

To this point the utility of an existing ITFDM and developed granular vulnerability assessment definition tables capable of providing a comprehensive assessment of an organization's MI vulnerabilities has been enhanced. Both concepts are now used to develop an MI vulnerability assessment process.

3.3.3 Malicious Insider Vulnerability Assessment (MIVA) Process. This section presents the assumptions, limitations, and nine steps of the MIVA process. The expanded ITFDM and common security element (PDR) definitions provide the framework for the development of the nine-step MIVA process table.

Assumptions. The MIVA process assesses the effectiveness of MI mitigation strategies that protect information owner's critical information. Therefore, MIVA assumes the following:

- Information owners have determined the subset of data that they deem the most critical, and
- Existing MI mitigation strategies intended to protect the information owner's critical information are in place.

Limitations. A known limitation of the MIVA process is the assignment of quantitative values based on a qualitative assessment process (use of PDR classification definition tables). The RRR qualitative to quantitative transformation technique is intended to provide information managers a more straightforward means of interpreting vulnerability assessment results. The problem is that information owners may assume that the values are quantitative when in reality they are not (calculations based upon ordinal scaling - high, medium, and low). The potential ramifications are not likely to be of significance due to the presentation of the quantitative values in an ordinal-based definition table. However, if the quantitative values were presented on their own (not in the ordinal definition table), the assessment results would likely be misleading.

MIVA Process Table. Table 3.5 presents the nine step MIVA process using the extended ITFDM as well as PDR definition tables. As described in the MIVA process table, every action listed under an information owner's MI intention of concern (identified using the ITFDM) is evaluated against the effectiveness of MI mitigation strategies. Each action receives its own vulnerability assessment score. The intention's vulnerability assessment score is the highest vulnerability assessment score of all possible listed methods of exploitation (i.e., malicious actions), listed in the ITFDM. The concept of assigning the root node (i.e., MI intention) the vulnerability value of the leaf node (i.e, malicious action) with the highest vulnerability is based upon the attack trees presented in Chapter II.

The first step of the MIVA process maps an organization's MI mitigation strategies to one or more of the applicable security practice elements. Table 3.6 is an example of the mapping of mitigation strategies to security practice elements.

Step three of the MIVA process calls for penetration testing which evaluates the effectiveness of the mitigation strategies to defend against MIs. MI mitigation strategies assessed as effective yield higher security levels and lower subsequent vulnerability levels whereas ineffective MI mitigation strategies yield lower security levels and higher subsequent vulnerability levels.

Table 3.5: Malicious Insider Vulnerability Assessment Process Steps

Step	Description
1	Map each mitigation strategy identified to the applicable security practice element(s) - PDR.
2	Assist the critical data stakeholder(s) in selecting intentions they perceive as potential insider threats from the insider threat functional decomposition model (ITFDM).
3	Use the ITFDM to identify the action(s) listed under each of the intentions identified in Step 2.
4	Using a typical system user account, attempt to exercise the first malicious action identified in Sstep 3. Based upon the ability to exercise the action, mitigation strategies, and vulnerability definition tables determine the given action's PDR security level (high, medium, or low).
5	Sort (low to high) and map the PDR security levels determined in Step 4 to the PDR vulnerability classification level table. The PDR vulnerability classification level table provides the corresponding weighted values for all possible PDR security level combinations.
6	Enter the data from Steps 2-5 into the malicious insider vulnerability and potential impact DSS.
7	Repeat Steps 4-6 for each action listed under the selected potential malicious insider intent identified in sStep 2.
8	The intentions resulting vulnerability security score is determined by the applicable action assessed with the highest weighted value and corresponding weighted value.
9	Repeat Steps 4-7 for each identified potential malicious insider intent identified by critical information owners in Step 2.

Table 3.6: Example Mapping for Step One of the MIVA Process

Critical Data Mitigation Strategies	Applicable Security Practices
Data Recovery Plan	Response
Encrypted Files	Prevention
Auditing	Detection and Response
Virus Protection	Prevention

3.3.4 Evaluation. The objective of the MIVA process is to provide critical data information owners with separate vulnerability assessments for each MI intention of concern. The perceived MI intention of concern varies depending upon the organization's mission and type of critical data. Providing information owners with a method of identifying applicable intentions of concern allows them to evaluate the effectiveness of mitigation strategies for only the most threatening MI intentions and associated actions to exploit their critical data.

3.4 Impact Assessment Process

Existing impact assessment frameworks do not provide information owners with an effective methodology to understand of the potential effect on their organization resulting from successfully performed MI actions [19, 27]. MI impact assessment results provide information managers with added insight on the value of their critical data. Information managers may use the MI potential impact results to aid in the mitigation strategy decision process.

This research uses a similar, but novel approach to develop an MI-specific impact assessment process that was used in the development of the MIVA process. The Malicious Insider Potential Impact Assessment (MIPIA) process (Section 3.4.1) develops and uses three definition tables whose results are aggregated into an overall impact assessment values. The MIPIA process component tables consist of separate CIA component tables, similar to the approach used by the National Institute of Standards Technology's (NIST's) information technology impact assessment model [11].

3.4.1 Approach. This research develops a MIPIA process that measures the potential impact of MI actions. A major variation of the MIPIA process is MIPIA process assesses only the malicious intentions of concern (not the associated actions) identified by information owners in the MIVA process. It is not necessary to assess the impact of each successfully performed malicious action, because they are only methods by which a given malicious intention can be performed. MIPIA provides impact assessment values for each of the individual MI intentions of concern identified by information owners (from the ITFDM).

Once each component of the CIA security objectives are assessed, the combined impact levels (vulnerability levels) are aggregated to determine the overall impact (illustrated in Table 3.10). Successfully realized MI intentions do not always have a direct impact on each CIA component. Such is the case of the thumb drive example discussed earlier using a thumb drive to download and subsequently distribute critical data in an unauthorized manner primarily impacts the confidentiality component of the three security objectives (CIA). In cases such as this, individual CIA components having little or no impact on a given MI intention would be assessed a low level.

Prior to developing the steps that comprise the MIPIA process, it is first necessary to define the common security objectives. The common security objectives classifications (CIA), depicted in Figure 3.4, are the foundation for the MIPIA process.

3.4.2 Common Security Objective Definition Tables. Similar to the NIST's impact assessment framework, an MI-specific impact assessment methodology using the CIA security objectives is used [11]. Individual CIA definition tables are critical elements in determining the MI impact levels in the MIPIA process. In each of CIA

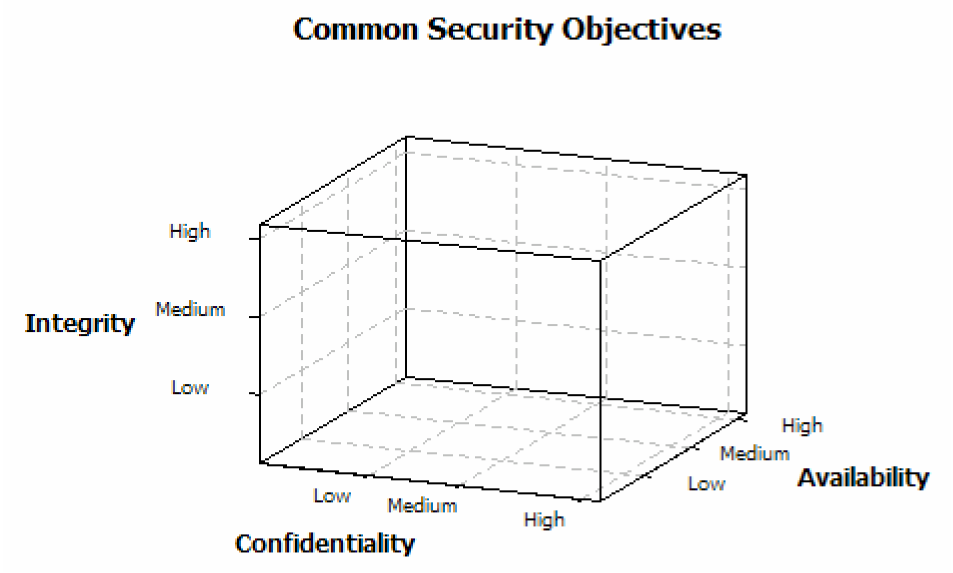


Figure 3.4: Security Objectives Impact Model.

component definition tables, the key words that separate high, medium, and low in each definition are *italicized*. The various definitions in each table are carefully modified impact assessment definition tables, used in existing research, to apply to the MI and CIA security objectives [11].

3.4.2.1 Individual CIA Definition Tables. The first CIA component, confidentiality, classifies impact levels according to the impact of successful MI actions have in the unauthorized access of critical data. Table 3.7 defines the three confidential classifications.

The second CIA component, integrity, classifies impact levels of successful MI actions that result in compromised and subsequently unreliable critical data. Table 3.8 defines the three integrity classifications.

The security levels for the last component in CIA, availability, are classified according to the impact of successful MI actions that cause critical data to be unavailable. Table 3.9 defines the three integrity classifications.

Table 3.7: Confidentiality Impact Level Definitions

Confidentiality Impact Level	Definition
High	Unauthorized access to critical data could result in *unrecoverable* financial losses, destroyed reputation, lost customers, or a major threat to national security.
Medium	Unauthorized access to critical data could result in *significant* financial losses, damaged reputation, lowered customer confidence, or a threat to national security.
Low	Unauthorized access to critical data could result in *minor* financial losses, slightly tarnished reputation, or threat to national security.

Table 3.8: Integrity Impact Level Definitions

Integrity Impact Level	Definition
High	Unreliable critical data, due to a malicious insider compromise, could result in *unrecoverable* financial losses, inability to accomplish essential missions, loss of life, or a major threat to national security.
Medium	Unreliable critical data, due to a malicious insider compromise, could result in *significant* financial losses, hindered ability to accomplish missions or tasks, or a threat to national security.
Low	Unreliable critical data, due to a malicious insider compromise, could result a *minor* hindrance to mission accomplishment or threat to national security.

Table 3.9: Availability Impact Level Definitions

Availability Impact Level	Definition
High	Unavailable data could result in *substantial* financial losses, inability to accomplish essential missions, tarnished reputation, loss of life, or a major threat to national security.
Medium	Unavailable data could result in *significant* financial losses, hindered ability to accomplish missions or tasks, loss of life, or a threat to national security.
Low	Unavailable data could result in *minor* financial losses and/or customer annoyance, or threat to national security.

3.4.2.2 Aggregate PDR Security Level Definition Table. Table 3.10 aggregates the assessed security level results in order from lowest to highest potential impact level for each of the CIA component tables (Tables 3.7-3.9). Again, the key words that separate the impact levels in each definition are *italicized*.

3.4.2.3 Classification Levels. Similar to the MIVA process, the aggregated CIA security level table includes two sub-classification levels within the high category (i.e,. high and very high), in order to provide further distinction between assessed CIA aggregated scoring. Higher assessed CIA component potential impacts from successfully realized MI intentions result in a higher potential impact in the combined CIA definition table.

3.4.2.4 Vulnerability Level Value Weighting. The MIPIA process applies the same value weighting principles discussed earlier in the MIVA process (3.3.2.4). The MIPIA aggregated CIA table (Table 3.10) contains ten possible outcomes. The CIA table uses the same rank reciprocal rule approach, presented in the MIVA process, to assign discrete weighted values to individual CIA security levels. It can be seen in Table 3.10 that corresponding weighted vulnerability values increase as the impact levels increase.

Table 3.10: Combined CIA Impact Classifications Definitions with Corresponding Individual CIA Vulnerability Level Possibilities

Potential Impact Level	Impact Definitions
Very High Impact High-High-High (0.34) High-High-Medium (0.17)	The potential impact of malicious insider actions to critical data, when measured against the three common information assurance classifications, could be *detrimental in varying degrees* within this category in terms of financial losses, inability to accomplish essential missions, loss of life, or a major threat to national security.
High Impact High-High-Low (0.11) High-Medium-Medium (0.09) High-Medium-Low (0.07) High-Low-Low (0.06)	
Medium Impact Medium-Medium-Medium (0.05) Medium-Medium-Low (0.045) Medium-Low-Low (0.035)	The potential impact of potential malicious insider actions to critical data, when measured against the three common information assurance classifications, could be *significant in varying degrees* within this category in terms of financial losses, hindered ability to accomplish missions or tasks, or a threat to national security.
Low Impact Low-Low-Low (0.03)	The potential impact of potential malicious insider actions to critical data, when measured against the three common information assurance classifications, could be *minimal* within this category in terms of financial losses, hindered ability to accomplish missions or tasks, or a threat to national security.

3.4.2.5 Evaluation. The CIA impact level definition table have a greater level of robustness than existing impact assessment frameworks thus allowing for a more comprehensive insider threat potential impact assessment. The development of the CIA definition tables used many of the same approaches as PDR definition tables. The major differences between the PDR and CIA definitions is PDR definitions are based on common security elements that assess the effectiveness of MI mitigation strategies, while the CIA definitions are based on common security objectives that assess the potential impact of MI realized malicious intentions.

The following four-step MIPIA process uses the component table and aggravated CIA definitions to determine the potential impact on a given organization for each of the same malicious intentions of concern identified by information owners in the MIVA process.

3.4.3 Malicious Insider Potential Impact Assessment (MIPIA) Process. This section presents the assumptions, limitations, and four steps of the MIPIA process.

Assumptions. The MIPIA process assesses the impact of realized malicious intentions. Therefore, MIPIA assumes:

- The organization has previously performed a MIVA
- The MIPIA process assesses the same malicious intentions of concern identified during the given organization's MIVA
- Each of the assessed malicious intentions of concern can be successfully realized (one or more possible action can be performed)

Limitations. As with the MIVA process, the MIPIA process assigns quantitative values to a qualitative assessment process (use of CIA classification definition tables). While based on a qualitative process, quantitative values provide information owners with a more tangible means of determining the potential impacts of successfully realized MI intentions as opposed to those that qualitative classifications results can provide.

MIPIA Process Table. Table 3.11 presents the four-step MIPIA process that assesses he malicious intentions of concern identified in the MIVA process. Each malicious intention of concern receives its own vulnerability assessment score.

Table 3.11: Malicious Insider Potential Impact Assessment Process Steps

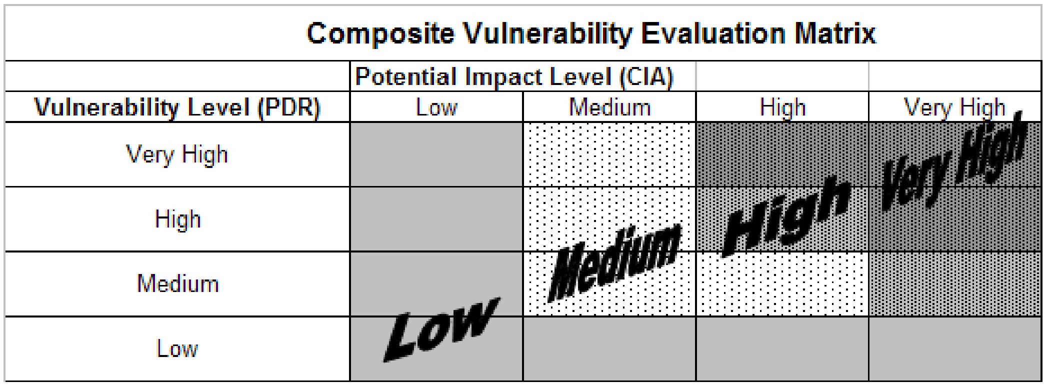
Step	Description
1	Take the first intention identified in the MIVA process and use the security objectives description tables to classify the potential impact on confidentiality, integrity, and availability (CIA) operating under the assumption that one or more of the actions within the malicious intention can be successfully performed.
2	Sort (high to low) and map the CIA potential impact levels determined in Step 1 to the CIA potential impact table. The CIA potential impact classification level table provides the corresponding weighted values for all possible CIA impact level combinations.
3	Enter the results from Steps 1 and 2 into Decision Support System (DSS).
4	Repeat Steps 1-3 for each malicious intention of concern evaluated in the MIVA process.

3.4.4 Evaluation. The objective of the MIPIA process is to provide critical information owners with separate impact assessments for each MI intention that poses a threat to their critical data. The MIPIA process results also provide information managers with added insight to value of their critical data.

3.5 Malicious Insider Composite Vulnerability

Once an organization performs the MIVA and MIPIA processes, the results can be fused to provide a composite vulnerability assessment for each MI intention of concern. The composite vulnerability MI intention assessment serves as a valuable data point in the data mitigation strategy decision process.

3.5.1 Composite Vulnerability Matrix. Figure 3.5 provides information owners with critical information composite MI vulnerability levels. The table determines the composite MI vulnerability for each malicious intention based upon the given intention's assessed vulnerability and impact classification levels intersection.



Composite Vulnerability Evaluation Matrix

	Potential Impact Level (CIA)			
Vulnerability Level (PDR)	Low	Medium	High	Very High
Very High				
High				
Medium				
Low				

Very High
High
Medium
Low

Figure 3.5: Composite Vulnerability Matrix.

A vulnerability assessment level of very high paired with a potential impact assessment level of low results in an overall composite vulnerability of low (information owners may likely assume the given intentions composite vulnerability). A vulnerability assessment level of medium paired with a potential impact level of results in an overall high composite vulnerability of very high. In this case, information owners may likely choose not to accept the risk and add additional mitigation strategies to lower the vulnerability level and subsequent composite vulnerability classification level.

3.5.2 Evaluation. Composite MI vulnerability levels, as determined in the Figure 3.5, enable information owners to understand their vulnerability and potential impact levels for each MI intention. Information owners may add mitigation strategies as needed to lower the overall vulnerability. Composite vulnerability levels can be reassessed after MI mitigation strategies are added. Providing that information owners select effective additional MI mitigation strategies to protect against a given malicious intention, the intentions composite vulnerability classification levels should decrease when reassessed.

3.6 Decision Support System

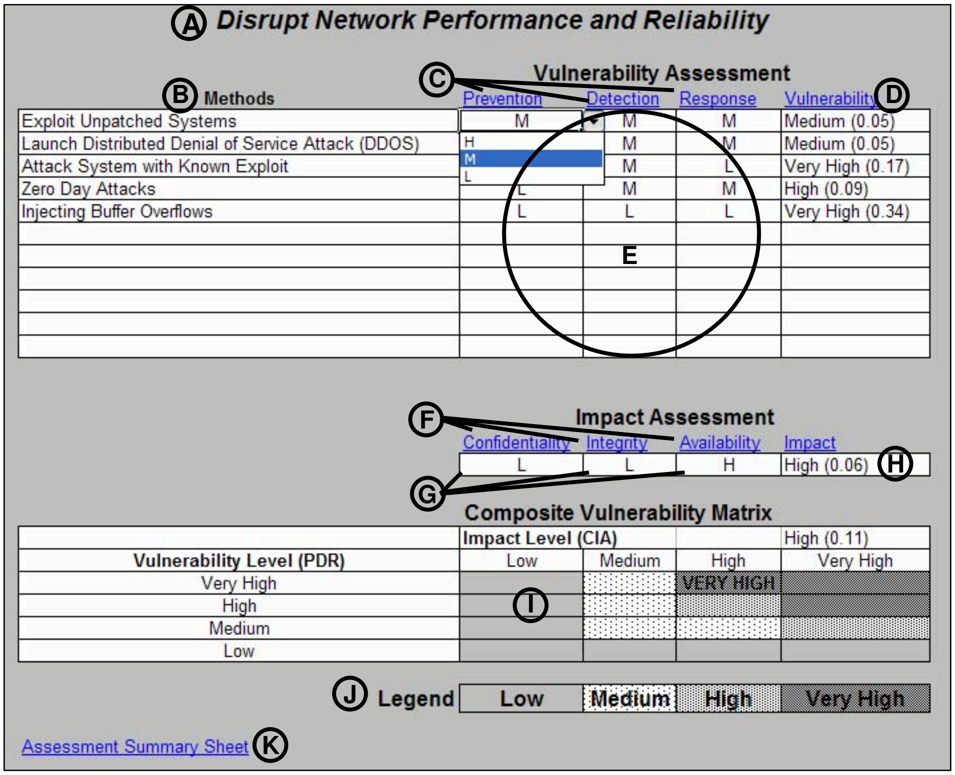
This section discuses a MI Decision Support System (DSS) that captures the output from this research's proposed vulnerability and impact assessment methodology and provides information owners with insider threat composite vulnerability levels.

3.6.1 Background. A DSS is, "a computer-based system that aids the process of decision-making" [12]. DSSs can be either *active, passive, or cooperative* [17,26]. The passive form of DSS is used to demonstrate the usefulness of the proposed concept. While active DSSs provide decision suggestions, passive based DSS's do not. However, passive DSS's still provide information owners with insight for the decision analysis process.

3.6.2 Approach. The proof-of-concept tool was developed with Microsoft Excel 2003. The primary purpose of developing the tool was to provide a simple MI critical information assessment tool that incorporates extended ITFDM, MI vulnerability, and MI composite vulnerability assessments.

3.6.3 Individual MI Intentions Assessment Worksheets. The DSS tool began with a single MI Excel worksheet based upon one of the sixteen common MI intentions (originating from the extended ITFDM). Upon final development of the worksheet, fifteen additional copies are to be made from the original MI intention worksheet (to capture all sixteen malicious intentions from the ITFDM). The intention header and corresponding methods of exploitation (applicable actions listed in the ITFDM) are modified accordingly.

3.6.3.1 Graphical User Interface and Functionality. The Graphical User Interface (GUI) of the malicious intention worksheet incorporates malicious intention and associated actions as well as MI vulnerability, impact, and composite vulnerability assessment. Figure 3.6 is a screenshot of the disrupt network performance and reliability worksheet that resides within the tool. To demonstrate the working application of the tool, the PDR and CIA dropdown boxes are populated with ran-



Disrupt Network Performance and Reliability

Vulnerability Assessment

Methods	Prevention	Detection	Response	Vulnerability
Exploit Unpatched Systems	M	M	M	Medium (0.05)
Launch Distributed Denial of Service Attack (DDOS)		M	M	Medium (0.05)
Attack System with Known Exploit		M	L	Very High (0.17)
Zero Day Attacks	L	M	M	High (0.09)
Injecting Buffer Overflows	L	L	L	Very High (0.34)

Impact Assessment

Confidentiality	Integrity	Availability	Impact
L	L	H	High (0.06)

Composite Vulnerability Matrix

	Impact Level (CIA)			High (0.11)
Vulnerability Level (PDR)	Low	Medium	High	Very High
Very High			VERY HIGH	
High				
Medium				
Low				

Legend	Low	Medium	High	Very High

Assessment Summary Sheet

Figure 3.6: Proof-of-Concept Tool MI Intention Screenshot

dom assessment values (High, Medium, or Low). Table 3.12 provides descriptions of the functionality for the MI intention worksheet depicted in Figure 3.6.

3.6.4 Assessment Summary Worksheet.

The MI summary worksheet is a single Excel worksheet that summarizes the vulnerability results from each of the completed intentions worksheets. The summary worksheet is an inclusive view of existing MI composite vulnerability levels and also provides the added capability to drill down to the individual worksheets that populate the summary worksheet.

3.6.4.1 GUI and Functionality.

Figure 3.7 is a screen shot of the tools MI summary intention worksheet. The assessment values (overall impact, vulnerability, and composite vulnerability) have been populated with the disrupt network performance and reliability worksheet's completed MI vulnerability and impact assessments. The following list (A-C) explains the GUI and functionality of the MI intention worksheet in Figure 3.7.

Table 3.12: DSS Tool's Intention Worksheet Component Descriptions

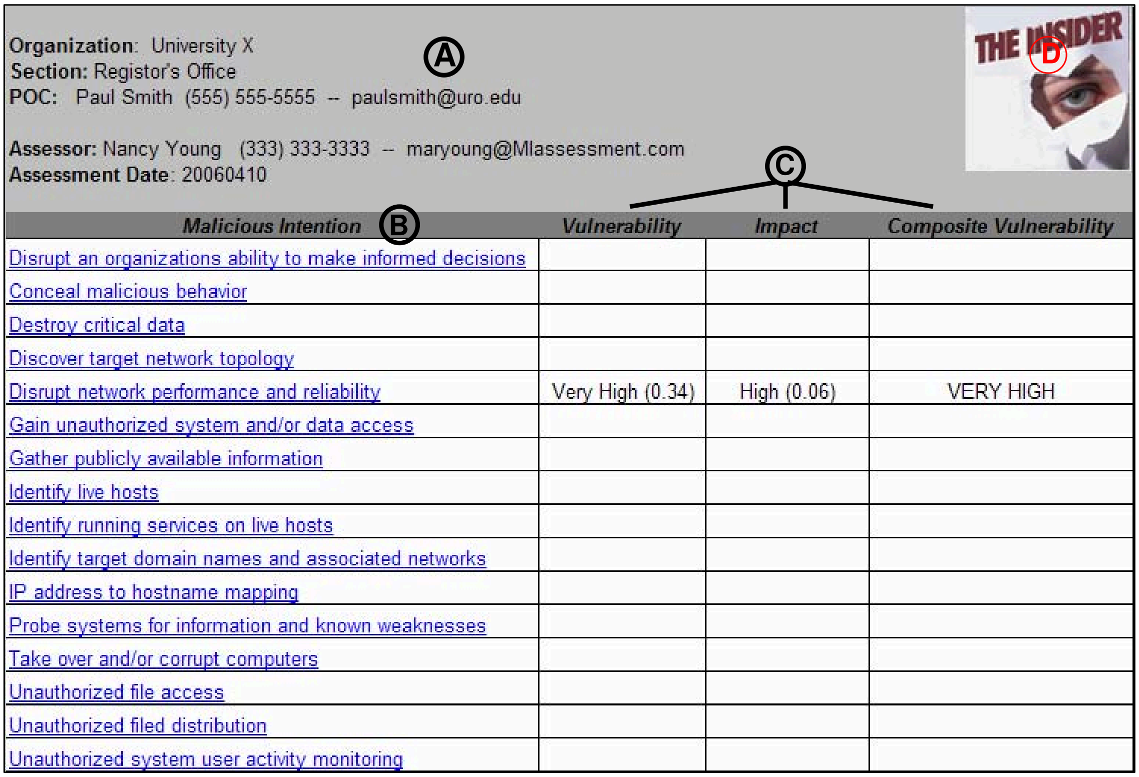
Figure Placement	Function
A	malicious intention (from ITFDM)
B	applicable methods (actions from ITFDM)
C	PDR component hyperlinks (to applicable MIVA definition tables
D	self populating MIVA process corresponding classification and weighted values (non-editable)
E	drop-down list boxes (High, Medium, Low)
F	CIA component hyperlinks (to applicable MIPIA definition tables)
G	drop-down list box's (High, Medium, Low)
H	self populating MIPIA process corresponding classification and weighted values (non-editable)
I	self populating composite vulnerability classification
J	composite vulnerability evaluation matrix legend
K	vulnerability assessment summary worksheet hyperlink

A - organization's and assessor's information

B - hyperlinks to the sixteen common MI individual intention's vulnerability and impact assessment worksheets (from ITFDM)

C - directly populated from each of the completed MI intention worksheets

The organization and assessor information at the top of the form is the only editable portion of the form. Each of the listed MI intentions (from ITFDM) are hyperlinks that enable users to go to any one of the sixteen individual malicious intention worksheets.



Organization: University X
Section: Registor's Office
POC: Paul Smith (555) 555-5555 -- paulsmith@uro.edu

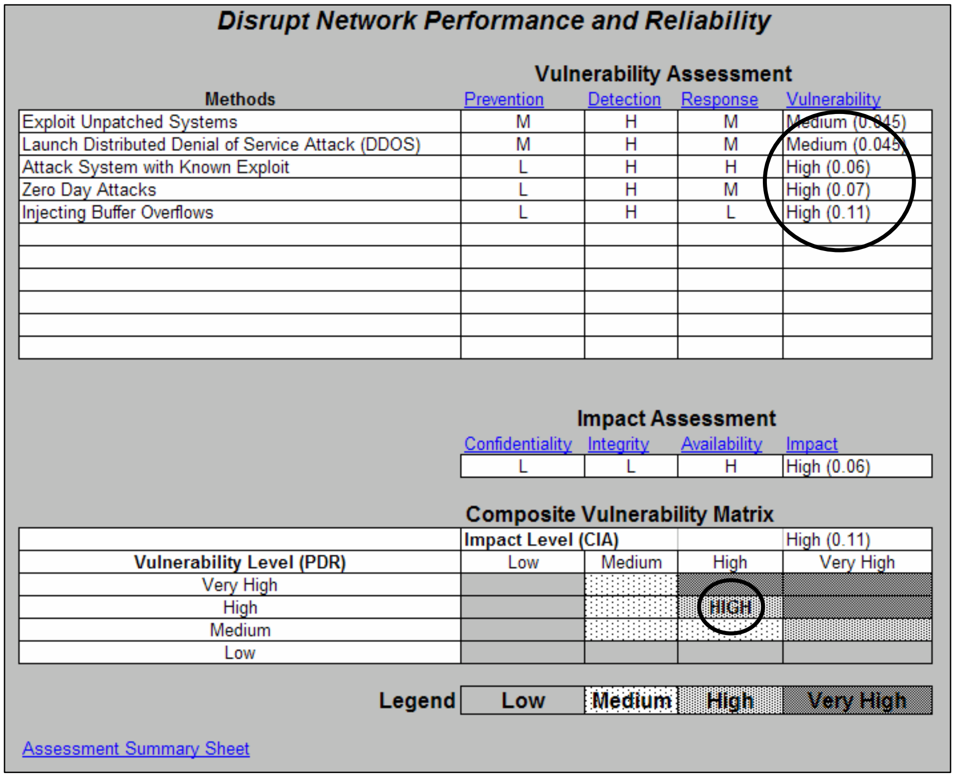
Assessor: Nancy Young (333) 333-3333 -- maryoung@MIassessment.com
Assessment Date: 20060410

Malicious Intention	*Vulnerability*	*Impact*	*Composite Vulnerability*
Disrupt an organizations ability to make informed decisions			
Conceal malicious behavior			
Destroy critical data			
Discover target network topology			
Disrupt network performance and reliability	Very High (0.34)	High (0.06)	VERY HIGH
Gain unauthorized system and/or data access			
Gather publicly available information			
Identify live hosts			
Identify running services on live hosts			
Identify target domain names and associated networks			
IP address to hostname mapping			
Probe systems for information and known weaknesses			
Take over and/or corrupt computers			
Unauthorized file access			
Unauthorized filed distribution			
Unauthorized system user activity monitoring			

Figure 3.7: Proof of Concept Tool MI Summary Screenshot

3.6.5 MIVA and MIPIA Process Verification. The purpose of this section is to verify that the MIVA and MIPIA processes as well as the proof-of-concept tool's automated calculations perform as intended. Adding additional MI mitigation strategies should result in a reduction in a previously assessed MI intention's vulnerability classification level. The MI intention's composite vulnerability classification (composite vulnerability matrix) should also be reduced.

The MI composite vulnerability classification level for a given intention is derived from the MIVA process (malicious action with highest vulnerability) and the MIPIA process (impact of exercised MI intentions). While an organization can not lower the potential impact without reducing current capabilities, MI intention's composite vulnerability classification levels can be reduced by decreasing MI vulnerability levels (PDR) assessed in the MIVA process.



Disrupt Network Performance and Reliability

Vulnerability Assessment

Methods	Prevention	Detection	Response	Vulnerability
Exploit Unpatched Systems	M	H	M	Medium (0.045)
Launch Distributed Denial of Service Attack (DDOS)	M	H	M	Medium (0.045)
Attack System with Known Exploit	L	H	H	High (0.06)
Zero Day Attacks	L	H	M	High (0.07)
Injecting Buffer Overflows	L	H	L	High (0.11)

Impact Assessment

Confidentiality	Integrity	Availability	Impact
L	L	H	High (0.06)

Composite Vulnerability Matrix

	Impact Level (CIA)			High (0.11)
Vulnerability Level (PDR)	Low	Medium	High	Very High
Very High				
High			HIGH	
Medium				
Low				

Legend	Low	Medium	High	Very High

Assessment Summary Sheet

Figure 3.8: Vulnerability Assessment and Tool Verification

Suppose the assessed organization in Figure 3.6 added additional MI mitigation strategies. The additional mitigation strategies provide real-time detection for each malicious method listed whose intentions are to disrupt network reliability and performance. Real-time detection would result in the re-categorization of actions' detection levels to high and subsequently lower vulnerability levels and associated weighted values for each action.

As previously noted, the method with the highest vulnerability is used to calculate the composite MI vulnerability level for the given intention. Adding real-time detection measures would lower each vulnerability level and subsequently passes a lower vulnerability classification level into the composite vulnerability matrix (Figure 3.8). In this case, the malicious intention's composite vulnerability is reduced from very high (Figure 3.6) to high (Figure 3.8), thereby verifying that the MIVIA and MIPA processes perform as intended. The proof-of-concept tool's classification and weighted value calculations also functioned as intended.

3.6.6 Tool Evaluation. The tool provides a computer-based method to perform composite vulnerability assessments. The tool does not provide suggested mitigation strategies to reduce MI intention vulnerability levels and subsequent composite vulnerability assessment levels.

However, the tool does a computer-based application that evaluates the effectiveness of MI mitigation strategies (assessed in the MIVA process). The tool also helps information owners understand the potential impacts of successful MI actions (assessed in the MIPIA process). Ultimately, critical information owners can use the composite vulnerability assessment results to assist in the MI mitigation strategy decision process.

The Composite Vulnerability Process Model (Figure 3.9) is a visual representation of the fundamental research methods developed in this research that are used to determine an organization's MI composite vulnerability levels.

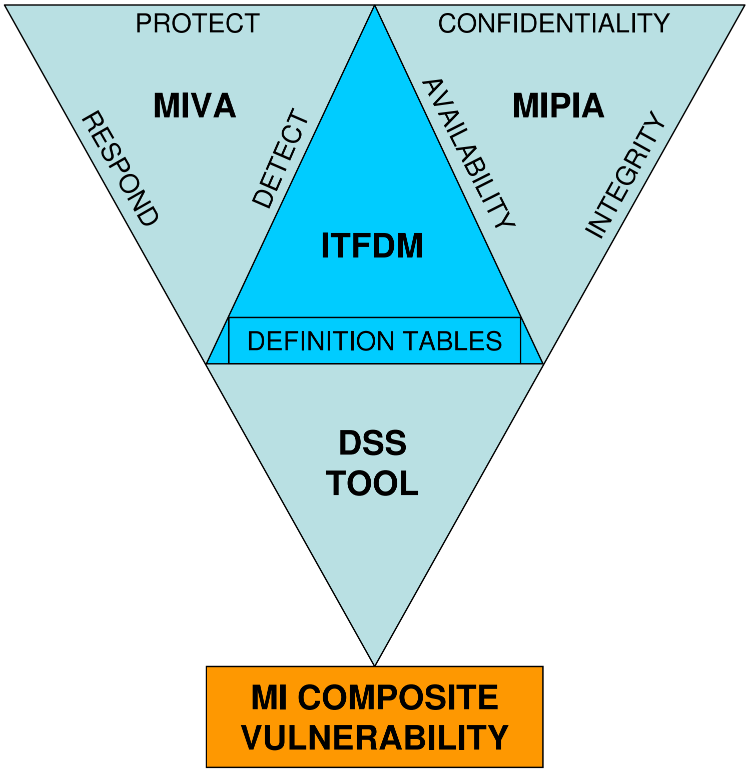


Figure 3.9: Vulnerability Assessment Process Model

3.7 Chapter Summary

This chapter discussed the fundamental concepts of this research including: (1) further decomposition of an existing insider threat model using malicious insider intentions and their associated actions; (2) content analysis of existing insider threat research to collect a variety of insider threat intentions and associated actions; (3) use of a multi-dimensional approach to develop malicious insider specific vulnerability and impact assessment process models; and (4) development of an DSS tool that serves as a working application of the fundamental concepts presented in this research. The next chapter contains a practical example that demonstrates the application of the concepts embodied in this research.

IV. Notional Example

This chapter presents a notional example to demonstrate the application of the concepts presented in this research to include: (1) the intent ITFDM, (2) MI composite vulnerability assessment process model, and (3) DSS tool.

4.1 Notional Example

To exercise the concepts proposed in this research and understand their potential, a notional example is developed. A generic organization is defined to demonstrate the wide applicability of the methodologies without limiting them to any one type of organization (e.g., commercial sector or Department of Defense).

4.1.1 Definitions. It will be beneficial to revisit key concepts that are used in the notional example.

- *Malicious Insider (MI).* Trusted users who intentionally use authorized information system access to perform unauthorized activities.
- *Organization.* Entities that share a common function and objective (e.g., finance, personnel office, intelligence office, registers office).
- *Typical system user.* Non-technical users who are trusted, possess authorized access to the system, but do not have administrator privileges.
- *Information owner.* System users who are, "... responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own" [11].
- *Critical data.* Data that has the greatest value to the information owners such as intellectual property, client information, and classified material. The greatest harm to the organization would occur if critical information is compromised.
- *Insider Threat Functional Decomposition Model (ITFDM).*) Definable taxonomy that systematically decomposes malicious insiders according to known MI intentions and associated actions.

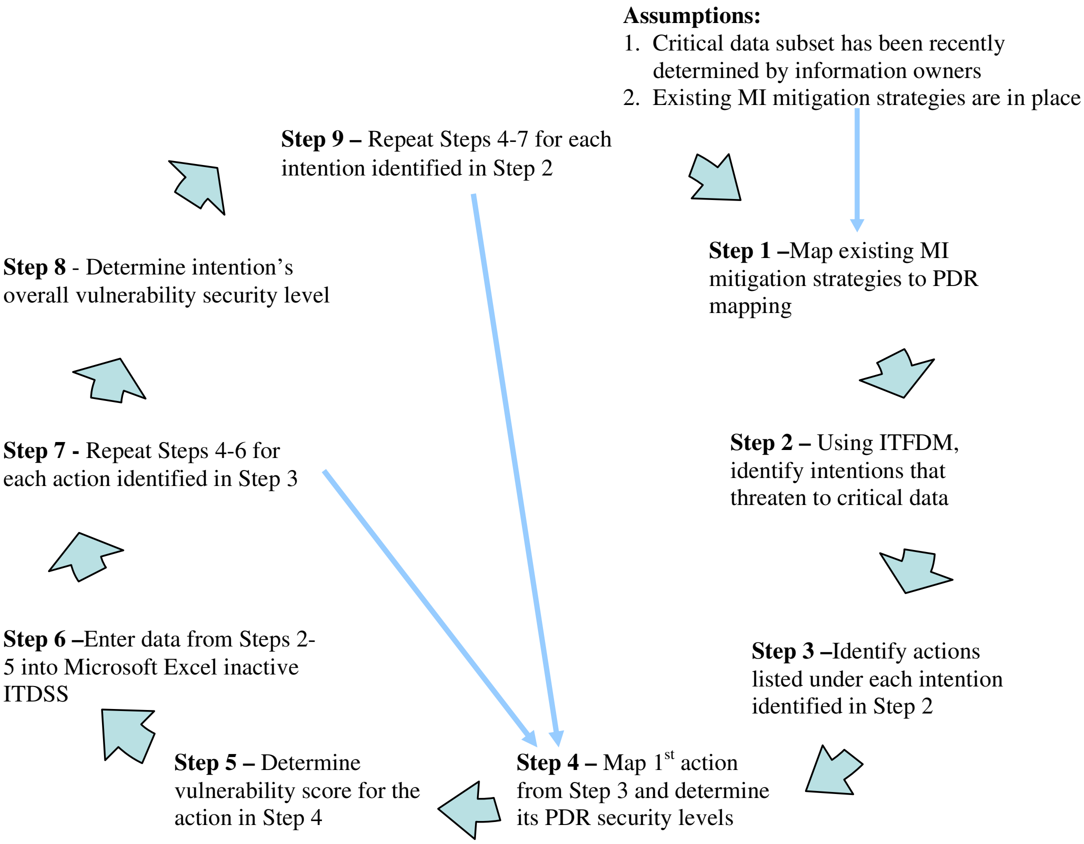

Assumptions:
1. Critical data subset has been recently determined by information owners
2. Existing MI mitigation strategies are in place
Step 1 –Map existing MI mitigation strategies to PDR mapping
Step 2 – Using ITFDM, identify intentions that threaten to critical data
Step 3 –Identify actions listed under each intention identified in Step 2
Step 4 – Map 1st action from Step 3 and determine its PDR security levels
Step 5 – Determine vulnerability score for the action in Step 4
Step 6 –Enter data from Steps 2-5 into Microsoft Excel inactive ITDSS
Step 7 - Repeat Steps 4-6 for each action identified in Step 3
Step 8 - Determine intention's overall vulnerability security level
Step 9 – Repeat Steps 4-7 for each intention identified in Step 2

Figure 4.1: MI Vulnerability Assessment Process Model.

- *Malicious Insider Vulnerability Assessment (MIVA).* Nine-step process that measures the effectiveness of an organization's MI mitigation strategies and subsequent insider threat vulnerability levels. Figure 4.1 graphically illustrates the process.

- *Malicious Insider Potential Impact Assessment (MIPIA).* Four-step process that analyzes the potential impact should MIs successfully exploit the organizations critical data. Figure 4.2 presents a graphical representation to illustrate the process.

- *Composite Vulnerability.* Determined by the combined MIVA and MIPIA process assessed results. Assessed composite vulnerability levels provide information owners with an organizations overall MI risk level for each malicious intention of concern.

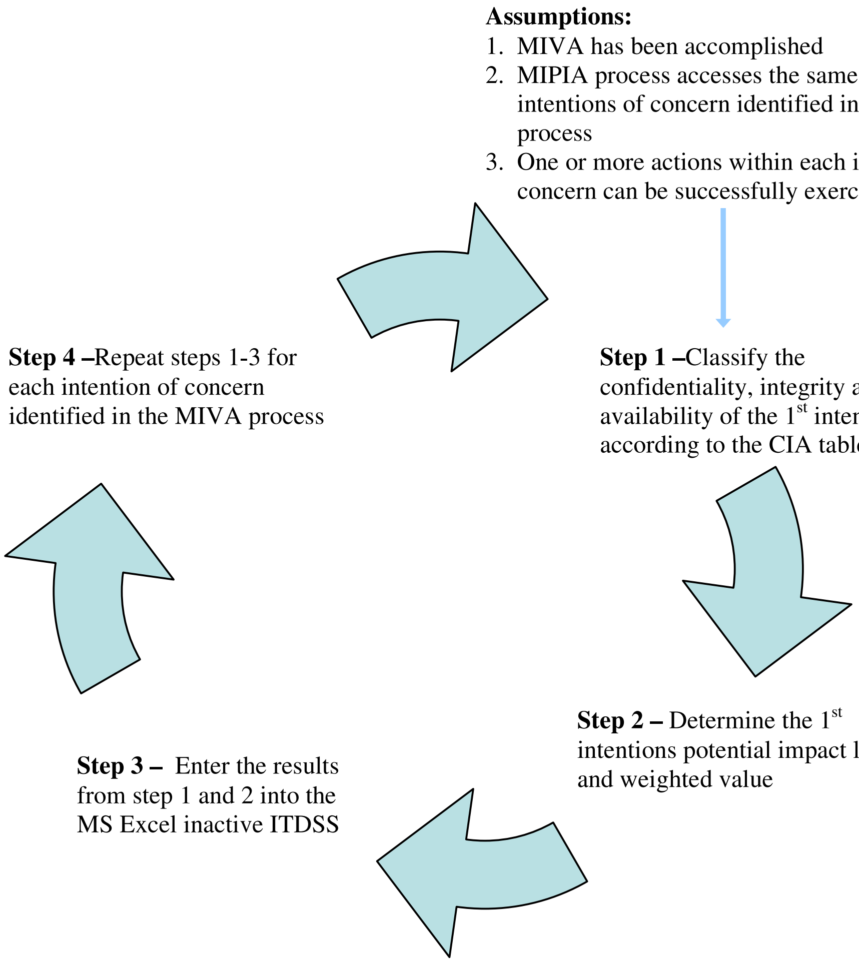

Assumptions:
1. MIVA has been accomplished
2. MIPIA process accesses the same malicious intentions of concern identified in the MIVA process
3. One or more actions within each intention of concern can be successfully exercised
Step 1 –Classify the confidentiality, integrity and availability of the 1st intention according to the CIA tables
Step 2 – Determine the 1st intentions potential impact level and weighted value
Step 3 – Enter the results from step 1 and 2 into the MS Excel inactive ITDSS
Step 4 –Repeat steps 1-3 for each intention of concern identified in the MIVA process

Figure 4.2: MI Potential Impact Assessment Process Model.

4.2 Notional Example Problem Definition

Suppose an organization must secure client accounts and personal information has requested an MI composite vulnerability assessment. The organization's objective is to assess the effectiveness of existing MI mitigation strategies and to obtain composite vulnerability assessment measurements they can use in the MI risk mitigation decision process. The following sections demonstrate the application of the processes developed in Chapter III.

4.2.1 Pre-Assessment Data Collection. The MIVA process needs two pieces of information prior to its use. First, information owners must have recently identified the subset of data that they deem most critical. Secondly, they must also identify candidate MI mitigation strategies to protect that critical information.

- *Critical data.* The organization identifies customer account numbers as well as personal data that could identify customers and employees as the organization's most critical data. Compromise of either of two sets of critical data would cause the greatest amount of harm to the organization.
- *Mitigation strategies.* Table 4.1 lists the MI mitigation strategies to protect the organization's critical data along with a brief explanation of each strategy.

4.2.2 MIVA. The MIVA process is to be performed independently for the various MI intentions of concern identified by information owners. However, for the sake of brevity, the vulnerability assessment methodologies can be sufficiently demonstrated by performing a composite vulnerability assessment using only one of the malicious intentions of concern identified by critical information owners.

4.2.2.1 Application of the MIVA Process. Since the organization requesting a composite vulnerability assessment has identified its most critical data as well as the mitigation strategies that are available to protect the critical data, the composite vulnerability assessment methodology can begin. The MIVA process is performed first to determine the effectiveness of the mitigation strategies and subsequent vulnerability levels.

Step 1. The first step maps each of the organizations mitigation strategies to the applicable security practice element (prevention, detection, and/or response - PDR). Table 4.1 is the mapping of the organization's mitigation strategies to the applicable PDR component.

Upon initial review of the organization's mitigation strategies in Table 4.1, it appears that the organization is focused primarily on protecting critical data through preventive measures. The organization lacks robustness in detection and response measures. However, the quantity of MI PDR component mitigation methods does not

Table 4.1: Notional Example: Mitigation Strategies to PDR Mapping

Mitigation Strategy	Description	Security Element
Privacy Act Training	Annual training to familiarize system users with the proper handling of client and employee information	Prevention
Virus Protection	Organization-wide virus protection with automated updates to protect against emerging threats	Prevention
Strong Passwords	Since insiders are already potentially aware of the information system's username conventions, the use of strong passwords make it more difficult for other users to obtain another user's password	Prevention
Physical Access Controls	Cipher lock system in place to access server room	Prevention
Audit Trail	Critical data and system access logging	Detection
Data Backups	Nightly, weekly, and monthly critical data backups	Response
Recovery Plan	Recovery document (not routinely tested) that focuses on the recovery of critical data and servers	Response

necessarily indicate the level of robustness that each common security element (PDR) provides against insider threats. The MIVA process will now assess the effectiveness of each mitigation strategy.

Step 2. In the second step, critical data information owners identify (using the ITFDM) malicious insider intentions that pose the greatest risk to the organization's critical information. In this example, critical information owners have identified the following malicious intentions as most threatening to the organization's critical information:

- Destruction of critical data
- Unauthorized file distribution

- Unauthorized file access
- Unauthorized system user activity monitoring

Normally, the remaining seven steps in the model would be repeated independently for each of the malicious intentions of concern identified. Each malicious intention of concern would receive independent MI vulnerability, potential impact, and composite vulnerability assessment levels. However, the methodology is amply demonstrated using one of the above malicious intentions of concern. For the sake of brevity, this notional example will proceed by performing the MIVA and MIPIA process using one of the organization's MI intentions of concern: unauthorized system user activity monitoring.

Step 3. The third step uses ITFDM to identify and list malicious actions for the applicable malicious intention of concern in Step 1. The following malicious actions apply to the malicious intention of unauthorized system user activity monitoring:

- Install spyware
- Install a sniffer
- Install a keystroke logger
- Install surveillance software

Step 4. Steps four through six are repeated for each of the malicious actions from Step three. Step four attempts to perform the first malicious action using a typical user network account. PDR security levels are then determined by combining the ability or inability to accomplish the malicious action and each of the component PDR definition tables. The three PDR component tables are found in Tables 3.1, 3.2, and 3.3. Normally, each malicious action would be independently assessed (Steps 4-6), however, the malicious actions provided in Step three will be assessed simultaneously. The assessed PDR levels are:

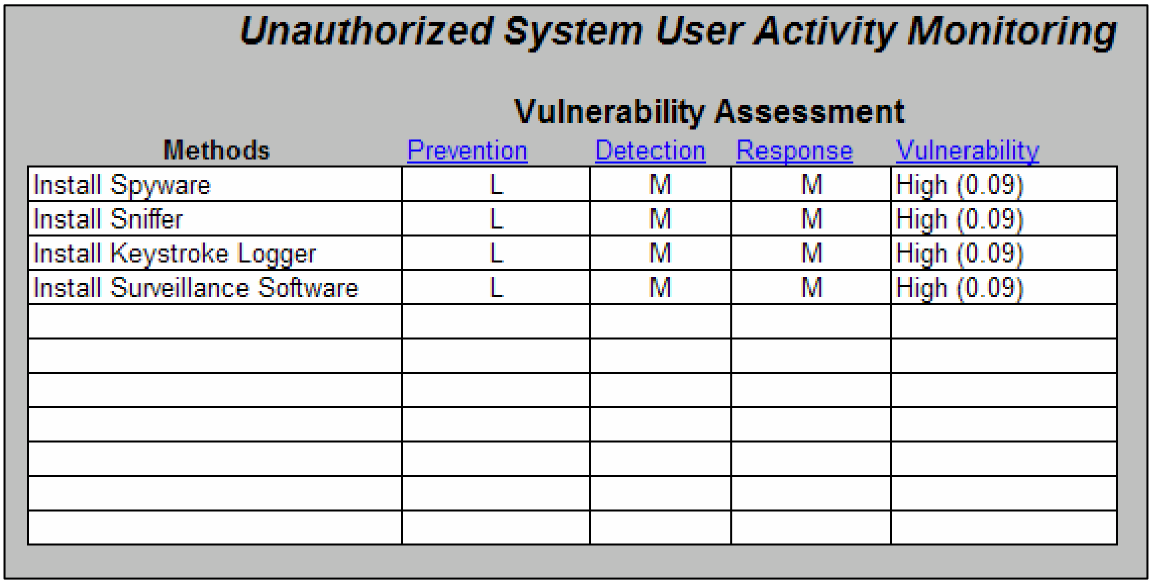
Assessed Prevention Security Level. Mitigation strategies do not prevent insiders with typical user accounts from installing spyware, sniffers, keystroke loggers, or surveillance software. Mapping these results to the prevention security table (Table 3.1) results in an assessed prevention security level of *low*. The organization needs additional mitigation strategies to prevent system users from performing unauthorized computer installations.

Assessed Detection Security Level. Mitigation strategies cannot detect insiders with a system user account who install unauthorized system monitoring software until after the malicious action has been performed. Mapping these results to the detection security table (Table 3.2) results in an assessed detection security level of *medium*. While the organization uses log files to detect a MI after the malicious action has been performed, the organization should consider implementing more robust MI detection methods for near real-time detection of MI exploit actions.

Assessed Response Security Level. The organization's primary means of responding to successful MI actions as defined in Table 4.1 is the use of routine data backups and recovery plans. However, the organization did not indicate the data backups are stored offsite, which means the backup tapes vulnerable to MI theft. The organization also did not indicate that the critical data and system recovery plans were routinely tested, verified, and updated. Mapping these results to the response security table (Table 3.3) results in an assessed detection security level of *medium*.

Step 5. This step determines each action's composite PDR classifications and corresponding weighted values. Due to the DSS tool in Step 6, this step can be omitted. The tool automates the production of composite PDR vulnerability results. In absence of the tool, this step would be manually determined (demonstrated later).

Step 6. In this step, the output from Steps 2-5 are entered into the DSS tool. Figure 4.3 illustrates the results from the vulnerability assessment portion of the tool, for individual and composite PDR levels as well as the corresponding weighted values for each malicious action. In most cases, it is unlikely each malicious action listed for a given malicious intention of concern would receive identical PDR assessment classification levels and subsequent composite PDR security levels. Like security level



Unauthorized System User Activity Monitoring

	Vulnerability Assessment			
Methods	Prevention	Detection	Response	Vulnerability
Install Spyware	L	M	M	High (0.09)
Install Sniffer	L	M	M	High (0.09)
Install Keystroke Logger	L	M	M	High (0.09)
Install Surveillance Software	L	M	M	High (0.09)

Figure 4.3: Notional Example: Vulnerability Assessment Results Screenshot

results for each of the four malicious actions in this notional example were primarily due to the similar method (unauthorized installations) used by each action to perform unauthorized system user activity monitoring.

In the absence of the DSS tool, the malicious intention's vulnerability level would be determined manually (Step 5 of the MIVA process). Figure 4.3 shows the process.

1. For each malicious action sort (low to high) their assessed PDR security levels
2. Map the sorted security levels (in the notional example low, medium, and medium) to the corresponding security levels in Table 3.4
3. Once the security levels are mapped, Table 3.4 provides the malicious action's MI vulnerability classification level and associated weighted value.

In the case of this notional example, mapping the PDR security levels of low, medium, and medium to Table 3.4 results in each action's vulnerability classification levels being assessed as *high* with a weighted value of *0.09* (since they all have the same assessed PDR security levels) .

The manual mapping of the notional example's MI security levels to Table 3.4 derived the same results as the DSS tool did. The like results for the manual method and automated method (MI proof-of-concept tool) of determining each malicious action's vulnerability levels and corresponding weighted values verify the correctness of the tool.

Steps 7-9. Steps 7-9 repeat Steps 4-8 (determine vulnerability levels) for each malicious intention of concern identified by critical data information owners in Step 1. Again, for practical purposes this notional example used just one of the malicious intentions of concern identified in Step 1 to demonstrate the methodology.

MIVA Results. Performing the MIVA process provides security level assessments for each malicious action. Higher security levels correlate to lower MI vulnerability levels, while lower security levels equate to higher MI vulnerability levels. Each action's associated malicious intention, provided by ITFDM, is assessed at the same vulnerability level as the action with greatest assessed vulnerability.

In this example, every associated action of the malicious intention of unauthorized system user activity monitoring were assessed simultaneously to determine vulnerability levels. Therefore, the malicious intention's vulnerability level (Figure 4.3) is assessed at *high* with a corresponding weighted value of *0.09*. The malicious intention's vulnerability level is one of the two components that determine the malicious intention's composite vulnerability level.

4.2.3 MIPIA.

Like the MIVA process, the MIPIA process performed independently for each of the various MI intentions of concern identified by information owners. For practical purposes, this notional example demonstrates the application of the MIPIA process by using the same malicious intention of concern (unauthorized system user activity monitoring) assessed in the MIVA process.

4.2.3.1 Application of the MIPIA Process.

The MIVA process assesses each individual method (i.e., action) of exercising a given malicious intention, the MIPIA process only assesses malicious intentions. The MIPIA process provides information owners with the adverse impacts resulting from an MI successfully achieving their malicious intentions.

At this juncture, it is beneficial to review the step prior to the application of the MIPIA process:

- The given organization has previously performed a MIVA
- The MIPIA process assesses the same malicious intentions of concern identified during the given organization's MIVA
- Each of the assessed malicious intentions of concern can be successfully realized (one or more possible action can be performed)

Step 1. The first step identifies each malicious intention's impact on each of the common security objectives (confidentiality, integrity, and availability - CIA) when an MI successfully achieves their malicious intention. Mapping each given malicious intention to the applicable classification levels defined in Tables 3.7, 3.8, and 3.9 provides potential impact levels for each CIA component.

Each malicious intention's overall potential impact is determined by aggregating the CIA component assessment results. The overall impact classification levels and corresponding weighted values are provided in Table 3.10. The malicious intentions overall impact classification level is derived automatically after each assessed CIA component's assessed classification levels are entered into the DSS tool. The tool's calculations are also based upon Table 3.10. A manual calculation of the malicious intent's overall impact is demonstrated later.

Proceeding with the notional example, CIA component potential impact assessments for the malicious intent of *unauthorized system user activity monitoring* are assessed as follows:

Assessed Confidentiality Impact Level. Of the three CIA components, confidentiality would be most adversely impacted if MIs were to install activity monitoring software such as keyloggers, sniffers, spyware, and other types of malicious software. Critical information could be completely compromised, which when mapped to the confidentiality definition table (Table 3.7), receives a potential impact level of *high*.

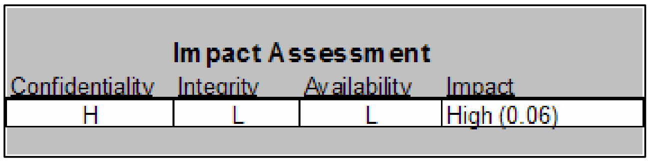
Assessed Integrity Impact Level. The malicious intention of *unauthorized system user activity monitoring* would not have a direct impact on the integrity of critical information. When mapped to the integrity definition table (Table 3.8), the malicious intention's integrity potential impact level to critical information is assessed as *low*.

Assessed Availability Impact Level. The malicious intention of *unauthorized system user activity monitoring* would also not have a direct impact on the availability of critical information. When mapped to the integrity definition table (Table 3.9), the malicious intention's availability potential impact level to critical information is assessed as *low*.

Confidentiality is the primary common security object (CIA) component impacted should an MI achieve the malicious intention of unauthorized system user activity monitoring. The confidentiality definition in Table 3.7 provides information owners insight to the potentially adverse impacts associated with an MI successfully installing unauthorized system user monitoring tools on organizational computers. Information owners can use the assessment results when determining which risk mitigation strategy to select to achieve an acceptable level of risk.

Step 2. This step determines each action's composite CIA classification levels and corresponding weighted values. Due to the use of the DSS tool in step 3, this step can be omitted. The tool determines composite CIA potential impact levels. In the absence of the tool, this step would be required (performed later in this section).

Step 3. This step enters the output from Step 1 into the MI DSS tool. Figure 4.4 illustrates the results from the potential impact assessment portion of the tool for individual and composite CIA levels as well as the corresponding weighted values for each malicious action.



Impact Assessment

Confidentiality	Integrity	Availability	Impact
H	L	L	High (0.06)

Figure 4.4: Notional Example: Potential Impact Assessment Results Screenshot

In the absence of the tool, the malicious intention's impact level would be determined manually (Step 2 of the MIPIA process). The following enumerated list manually calculated the assessed impact classification levels in this notional example:

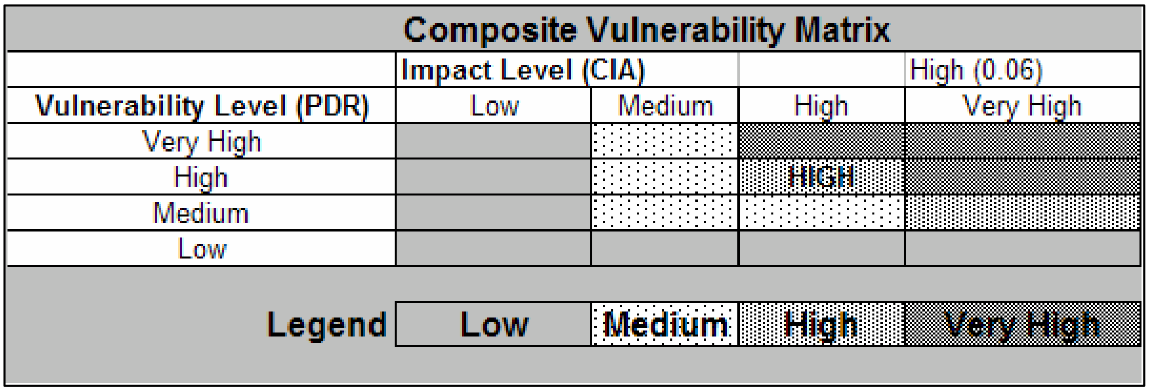
1. For each malicious action sort (high to low) assessed impact levels
2. Map the sorted impact levels (high, low, and low) to the corresponding impact levels in Table 3.10
3. Once the impact levels have been mapped, Table 3.10 provides the malicious action's aggregated MI impact classification level and associated weighted value.

Mapping the CIA impact levels of high, low, and low to Table 3.10 results in each action's impact classification levels being assessed as *high* with a weighted value of *0.06*.

The manual mapping of the notional example's MI impact classification levels to Table 3.10 derived the same results as the DSS tool and also verifies that the tool's calculations are correct.

Step 4. Step 4 repeats Steps 1-3 for each malicious intention of concern identified by the organization's information owners in Step 2 of the MIVA process. For practical purposes this notional example demonstrates the working application of the methodologies using one malicious intention of concern, thus satisfying Step 4.

MIPIA Results. The notional example demonstrated that MI actions do not necessarily impact each individual CIA component in the same manner (i.e, different classification levels). The individual CIA component definition tables (Tables 3.7,



Composite Vulnerability Matrix

	Impact Level (CIA)			High (0.06)
Vulnerability Level (PDR)	Low	Medium	High	Very High
Very High	░	▒	█	█
High	░	▒	▓ HIGH	█
Medium	░	▒	▒	▓
Low	░	░	░	░
Legend	░ Low	▒ Medium	▓ High	█ Very High

Figure 4.5: Notional Example: Composite Vulnerability Screenshot

3.9, and 3.8) provide the necessary granularity to account for the possible assessed between the CIA components.

The malicious intention's aggregated CIA component potential impact levels were assessed at *high* with a corresponding weighted value of *0.06*. The malicious intention's potential impact level is the second of the two elements that determine the malicious intention's composite vulnerability level.

4.2.4 Composite Vulnerability. Having performed the MIVA and MIPIA assessments for the information owner's MI intention of concern, *unauthorized system user activity monitoring*, the malicious intention's overall composite vulnerability level can be determined.

The MIVA process classifies the malicious intention as having a high vulnerability level. The MIPIA process then classified the malicious intention as having a high potential impact level. Mapping the vulnerability and potential impact assessment classification levels to the composite vulnerability matrix results in the malicious intention having a composite vulnerability classification level of *high*. Figure 4.5 illustrates the automated results from the composite vulnerability portion of the DSS tool. The organization is highly vulnerable to the information owner's concern of unauthorized system user activity monitoring and additional PDR mitigation strategies are necessary to lower the malicious intention's composite vulnerability classification level.

4.2.5 Vulnerability Assessment Verification.

The section adds additional mitigation strategies to the malicious intention from the notional example and re-assesses the malicious intentions vulnerability and subsequent composite vulnerability classification levels. It is expected that the malicious intention's vulnerability and subsequent composite vulnerability classification levels will decrease. Continued use of the MI DSS tool also provides a method to verify that the tool's formulas calculate as intended. This section will discuss only the MIVA steps affected by the re-assessment.

Table 4.2: Notional Example: Additional Mitigation Strategies

Mitigation Strategy	Description	Applicable Security Element
Group Policy	Implement system user group policy that prevents system users from installing software on organizational computers	Prevention
Commercial Software	Implement commercial software that prevents and detects users from installing software on organizational computers	Prevention and Detection

Upon review of the organization's mitigation strategies it is determined that the additional mitigation strategies in Table 4.2 would likely decrease the malicious intention's vulnerability classification levels:

The recommended additional MI mitigation strategies in Table 4.2 provide specific prevention and detection methods to decrease the vulnerability classification levels of the malicious intention of concern assessed in the example. Implementing group policies alone would provide a low cost means of improving security levels and subsequently lowering the malicious intention's vulnerability classification levels. However, commercial software can prevent typical users from installing software on organizational computers and also notifies information owners of typical users who attempt to install software (e.g., Watchdog). The combination of both of the two recommended additional mitigation strategies provides a layered approach that specifically addresses the information owner's concern of unauthorized system user activity monitoring. Typical system user's would be unable to perform software installations.

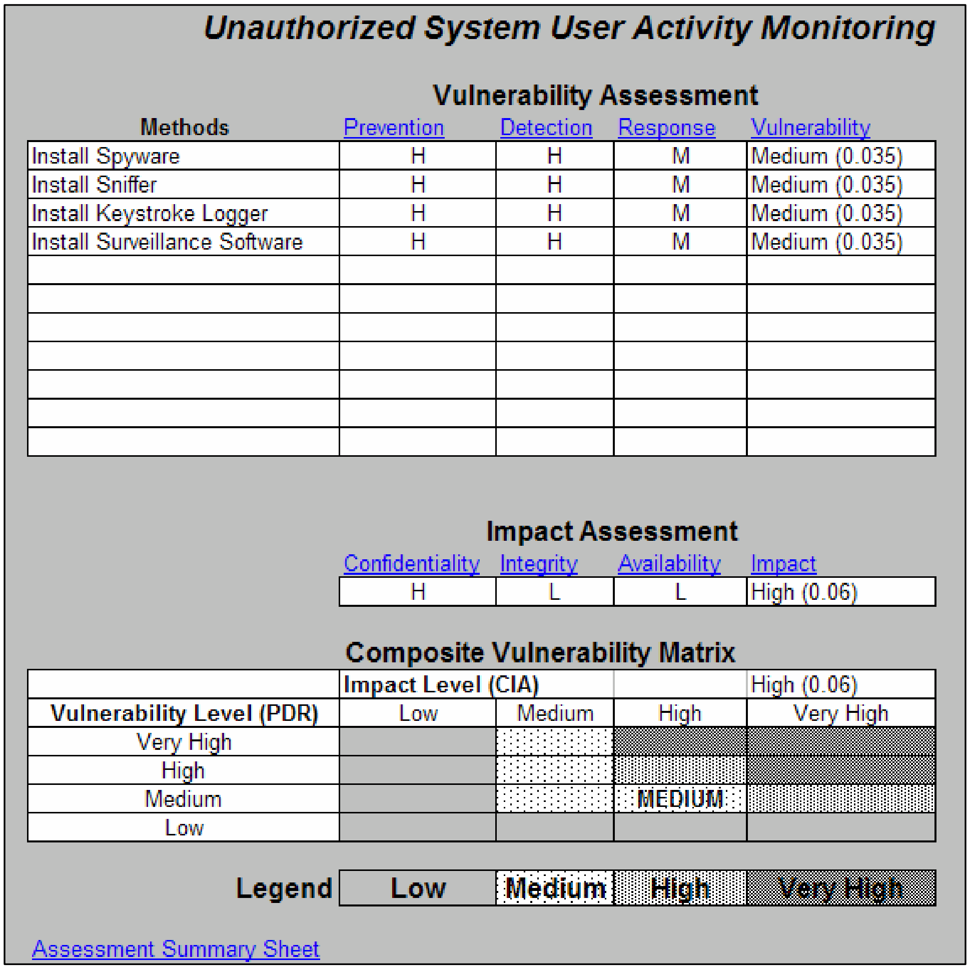
Assume the organization agreed and implemented the two recommended mitigation strategies. The recommended additional mitigation strategies apply to the prevention and detection security components which require repeating Steps 3-6 in the MIVA process to determine the new vulnerability classification levels.

4.2.5.1 Notional Example Vulnerability Re-Assessment. Mitigation strategies make it *highly unlikely* that users can perform installations on organizational computers. Mapping these results to the prevention security table returns a re-assessed prevention security level of *high*.

Re-Assessed Detection Security Level. Mitigation strategies now provide *near real-time discovery* of users attempting to perform installations on organizational computers. The commercial application's ability to detect typical system users who attempt to install software on organizational computers, coupled with existing audit trail capabilities, provide a layered approach to detecting typical system users attempting to circumvent security measures. Mapping these results to the detection security table results in a re-assessed detection security level of *high*.

Re-Assessment Results. Figure 4.6 shows the new vulnerability and composite vulnerability classification levels determined in the MIVA process during the reassessment. Implementing the two additional mitigation strategies resulted in the malicious intention's vulnerability classification level decreasing from *high* in Figure 4.3 to *medium* in Figure 4.6. The decrease in the malicious intention's vulnerability level was a direct result of the organization implementing the two additional mitigation strategies. The malicious intention's composite vulnerability classification level decreased from *high* in Figure 4.5 to *medium* in Figure 4.6.

As intended, the additional mitigation strategies in the notional example resulted in the increased security classification levels for the prevention and detection components of the common security elements. As a direct result of the improved



Unauthorized System User Activity Monitoring

Vulnerability Assessment

Methods	Prevention	Detection	Response	Vulnerability
Install Spyware	H	H	M	Medium (0.035)
Install Sniffer	H	H	M	Medium (0.035)
Install Keystroke Logger	H	H	M	Medium (0.035)
Install Surveillance Software	H	H	M	Medium (0.035)

Impact Assessment

Confidentiality	Integrity	Availability	Impact
H	L	L	High (0.06)

Composite Vulnerability Matrix

	Impact Level (CIA)			High (0.06)
Vulnerability Level (PDR)	Low	Medium	High	Very High
Very High				
High				
Medium			MEDIUM	
Low				

Legend	Low	Medium	High	Very High

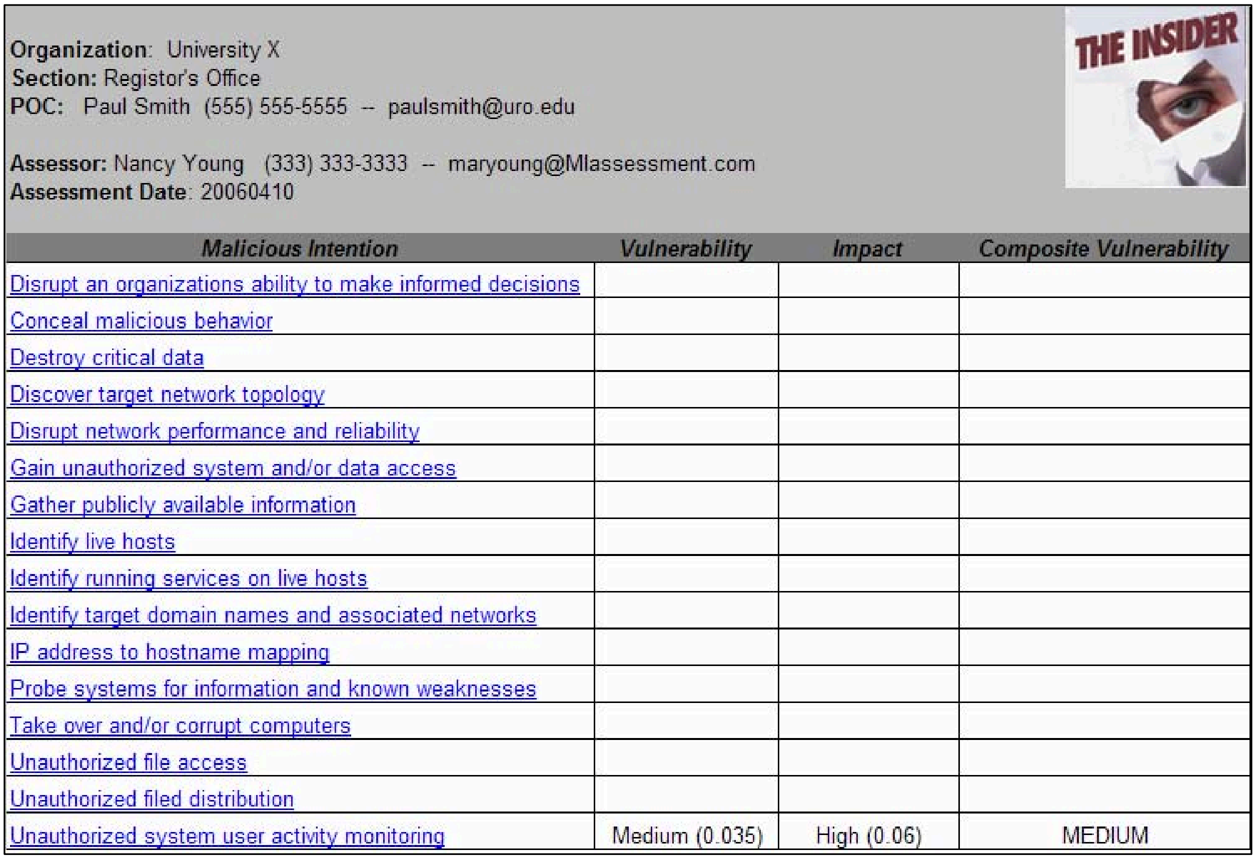
Assessment Summary Sheet

Figure 4.6: Notional Example: Re-Assessed Individual Worksheet

security PDR classification levels, the organization's vulnerability to the malicious intention of concern decreased as did the composite vulnerability. Figure 4.7 demonstrates the working summary MI worksheet from the DSS tool as applicable to this example. The tool performed as expected.

4.3 Chapter Summary

This chapter provides a notional example that demonstrates the fundamental concepts presented in this research. A generic organization's MI mitigation strategies are assessed using the MIVA process to determine the organization's vulnerability classification levels for a malicious intention of concern. The MIPIA process is per-



Organization: University X
Section: Registor's Office
POC: Paul Smith (555) 555-5555 -- paulsmith@uro.edu

Assessor: Nancy Young (333) 333-3333 -- maryoung@MIassessment.com
Assessment Date: 20060410

Malicious Intention	*Vulnerability*	*Impact*	*Composite Vulnerability*
Disrupt an organizations ability to make informed decisions			
Conceal malicious behavior			
Destroy critical data			
Discover target network topology			
Disrupt network performance and reliability			
Gain unauthorized system and/or data access			
Gather publicly available information			
Identify live hosts			
Identify running services on live hosts			
Identify target domain names and associated networks			
IP address to hostname mapping			
Probe systems for information and known weaknesses			
Take over and/or corrupt computers			
Unauthorized file access			
Unauthorized filed distribution			
Unauthorized system user activity monitoring	Medium (0.035)	High (0.06)	MEDIUM

Figure 4.7: Notional Example: Re-Assessed Summary Worksheet

formed to determine the malicious intention of concern's potential impact to the organization, should the intention be successfully exercised. The malicious intention's composite vulnerability classification level determines through mapping the MIVA and MIPIA results to the composite matrix. Additional mitigation strategies are applied and the malicious intention's vulnerability classification level is re-assessed. The re-assessment supported the expected results, which also verified the DSS tool performed as intended.

V. Conclusions and Recommendations

This chapter presents the research conclusions, significance, and recommended areas for future research.

5.1 Problem Summary

Identifying specific malicious actions authorized users can perform, pose a difficult problem for security personnel. An organization's inability to define the threats do to malicious insiders (MI) makes it difficult to assess the effectiveness of mitigation strategies and subsequently protect critical information from being exploited.

An insider threat malicious action taxonomy model is needed that organizations can use to identify MI actions of concern. Organizations also need to understand the impact of MI actions. Additionally, organizations need a method to assess the effectiveness of MI mitigation strategies. Knowledge of potential impact levels as well as the effectiveness of malicious insider mitigation strategies, will assist information owners in implementing mitigation strategies that provide an acceptable level of information risk.

5.2 Conclusions of this Research

The goals of this research were to extend and improve an existing insider threat taxonomy model and develop a composite vulnerability assessment process that can adequately determine an organization's current MI vulnerability levels.

5.2.1 Malicious Intent Driven Taxonomy Model. The ITFDM is further decomposed to characterize malicious intentions and associated actions. The extended ITFDM provides information owners with a framework to identify MI intentions of concern and associated actions. The extended ITFDM's enhanced robustness and adaptability is demonstrated through a notional example. This example illustrates how the improved model provides organizations a practical means of identifying potential malicious actions that pose a threat to their information and information systems.

5.2.2 Composite Vulnerability Assessment. This research introduces a framework for measuring MI vulnerability levels. The MIVA process provides a functional method for measuring the effectiveness of MI mitigation strategies. The MIVA process's focus includes: (1) critical information owners identifying MI intentions of concern and associated actions, and (2) assessing the effectiveness of MI mitigation strategies to prevent, detect, and respond to each malicious intention of concern. The usefulness of the MIVA process in assessing MI vulnerability is demonstrated by applying it to a particular scenario.

The MIPIA process provides critical information owners with a functional method to determine the impact of a MI succeeding. The MIPIA process includes assessing the potential impact to each of the common security objectives (confidentiality, integrity, and availability- CIA). The CIA assessment results are combined to determine a successfully performed malicious intention's overall potential impact. The usefulness of the MIPIA process in determining malicious intention's potential impact classification levels are illustrated through a notional example, demonstrating that the MIPIA process provides information owners a means of assessing the potential impact from successfully realized malicious actions.

5.3 Significance of this Research

Though not the primary focus of this research, the ITFDM was further decomposed to include malicious intentions and associated actions. Incorporating these components into the ITFDM significantly improved the model's robustness and usability.

This research also developed an MI vulnerability assessment methodology that enables information owners to: (1) identify malicious intentions of concern using the ITFDM, (2) determine the effectiveness of the organization's existing mitigation strategies via the MIVA process, (3) determine potential impact resulting from successful malicious actions via the MIPIA process, and (4) derive a composite vulnerability for the various malicious intentions of concern.

Unlike previous work, this research uses a granular approach by evaluating each security element (i.e., PDR) and objective (i.e., CIA) individually. This provides an aggregate level of risk assessment (i.e., vulnerability and impact assessment) that enables information owners to reduce MI risks to an acceptable level. In addition, the methodologies add quantitative values (using the rank reciprocal rule) to provide information owners a better sense of their organization's vulnerability levels than can be provided by qualitative values alone.

Additionally, this research developed an intuitive DSS tool that more precisely assesses the composite risk of an organizations information and information systems. The insider threat vulnerability assessment tool can be applied across various organizational domains to select appropriate MI mitigation strategies.

5.4 Recommendations for Future Research

5.4.1 Developing Threat-Based Variations to ITFDM. The expanded insider threat taxonomy model focused on malicious actions that could be performed by typical system users to carry out an employee's malicious intentions. The ITFDM could be further decomposed according to the various types of information system users (e.g., system administrator, contractors, system maintenance personnel, etc.). Further categorizing the threat could be achieved by developing separate ITFDM models for each threat (i.e.. information system users).

5.4.2 MI Vulnerability Assessment Values. This research used the rank reciprocal rule and definition tables to both quantify and qualify organization's MI threat levels. Future research could explore other methods of determining an organization's MI vulnerability levels that provide a more meaningful vulnerability assessment results.

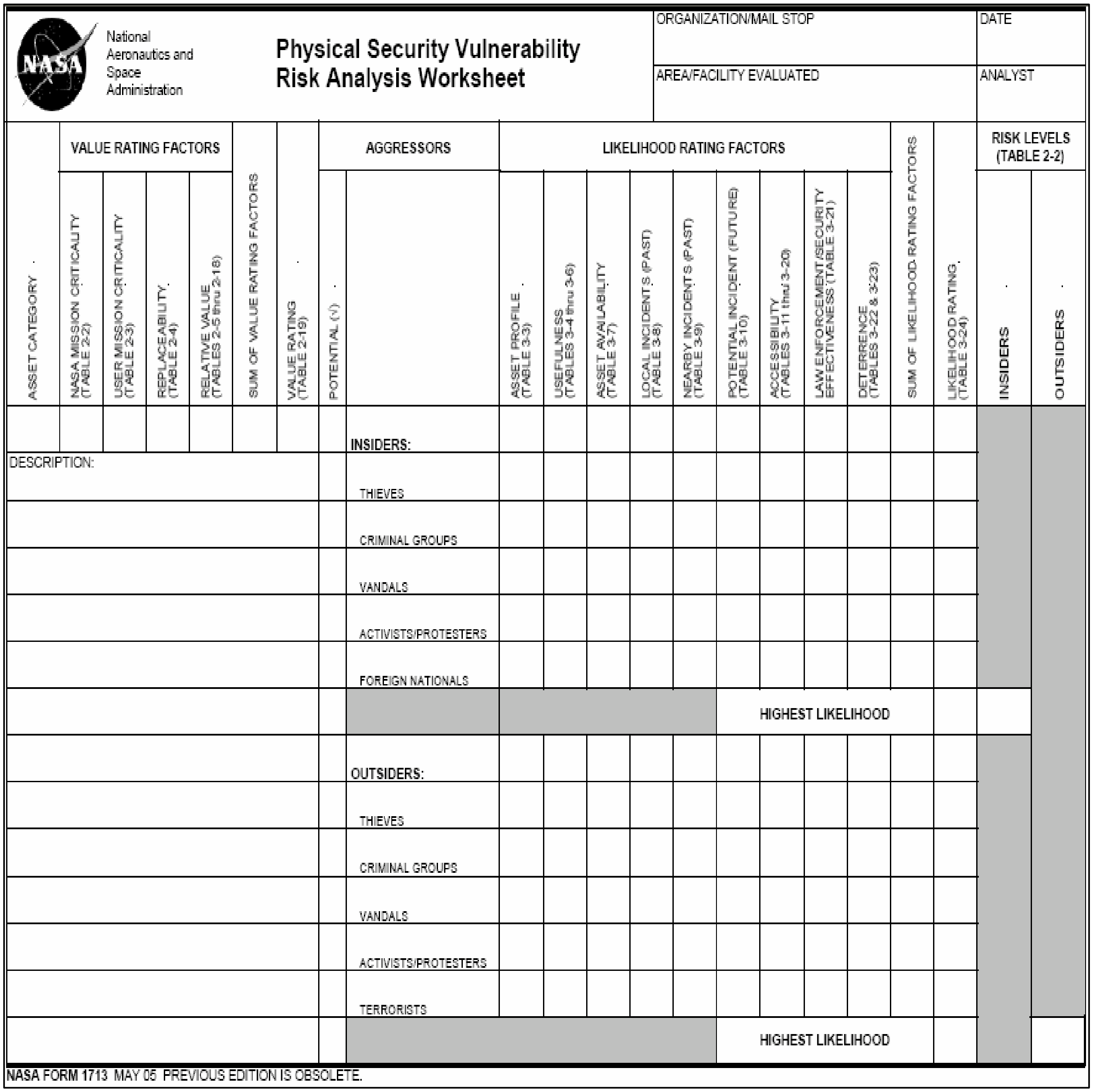
5.4.3 Extend Proof-of-Concept Tool. The proof of concept tool was developed to provide critical information owners with a working application that applies the fundamental MI vulnerability concepts from this research. The inactive-based DSS tool does not provide information owners with recommended MI mitigation strategies to lower an organizations residual risk. The tool could incorporate a active-based DSS approach that recommends applicable mitigation strategies according the assessed vulnerability levels. For example, if an organization's mitigation strategies MI response ability were assessed as low (i.e., high vulnerability), an improved active-based DSS tool could provide appropriate mitigation strategies to improve the MI response effectiveness and to decrease MI vulnerability levels.

5.5 Summary

This research provides information owners a MI vulnerability assessment methodology, along with a DSS tool to assess an organization's MI vulnerability levels. Furthermore, the vulnerability assessment methodology and tool's application can be applied across organizational domains (e.g., Department of Defense, e-business, or manufacturing).

Appendix A. NASA Physical Security Vulnerability Analysis Worksheet

NASA Form 1713.



National Aeronautics and Space Administration

Physical Security Vulnerability Risk Analysis Worksheet

ORGANIZATION/MAIL STOP

DATE

AREA/FACILITY EVALUATED

ANALYST

	VALUE RATING FACTORS							AGGRESSORS	LIKELIHOOD RATING FACTORS											RISK LEVELS (TABLE 2-2)	
ASSET CATEGORY	NASA MISSION CRITICALITY (TABLE 2-2)	USER MISSION CRITICALITY (TABLE 2-3)	REPLACEABILITY (TABLE 2-4)	RELATIVE VALUE (TABLES 2-5 thru 2-18)	SUM OF VALUE RATING FACTORS	VALUE RATING (TABLE 2-19)	POTENTIAL (√)		ASSET PROFILE (TABLE 3-3)	USEFULNESS (TABLES 3-4 thru 3-6)	ASSET AVAILABILITY (TABLE 3-7)	LOCAL INCIDENTS (PAST) (TABLE 3-8)	NEARBY INCIDENTS (PAST) (TABLE 3-9)	POTENTIAL INCIDENT (FUTURE) (TABLE 3-10)	ACCESSIBILITY (TABLES 3-11 thru 3-20)	LAW ENFORCEMENT/SECURITY EFFECTIVENESS (TABLE 3-21)	DETERRENCE (TABLES 3-22 & 3-23)	SUM OF LIKELIHOOD RATING FACTORS	LIKELIHOOD RATING (TABLE 3-24)	INSIDERS	OUTSIDERS
								INSIDERS:													
DESCRIPTION:								THIEVES													
								CRIMINAL GROUPS													
								VANDALS													
								ACTIVISTS/PROTESTERS													
								FOREIGN NATIONALS													
														HIGHEST LIKELIHOOD							
								OUTSIDERS:													
								THIEVES													
								CRIMINAL GROUPS													
								VANDALS													
								ACTIVISTS/PROTESTERS													
								TERRORISTS													
														HIGHEST LIKELIHOOD							

NASA FORM 1713 MAY 05 PREVIOUS EDITION IS OBSOLETE.

Figure A.1: NASA Physical Security Vulnerability Risk Analysis Worksheet

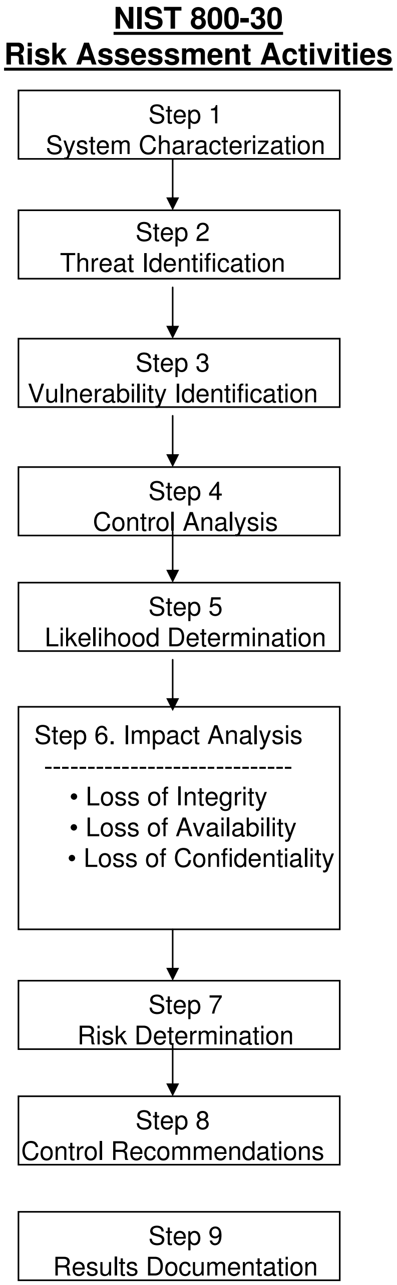


Figure B.1: Risk Assessment Methodology Flowchart

Appendix C. ITFDM: Action, Alteration, Snooping, and Elevation

These are the functionally decomposed MI four protection states models.

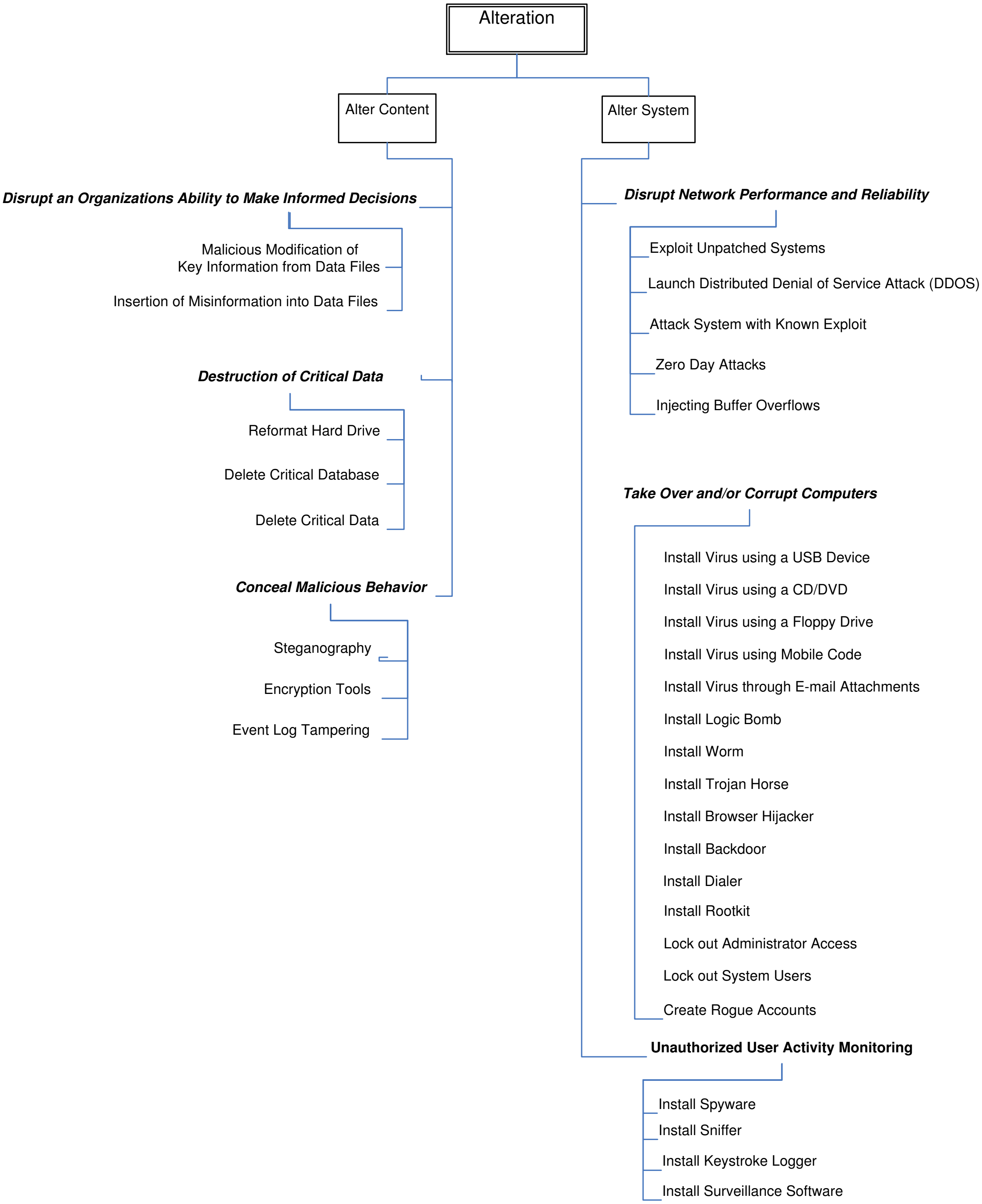

Alteration
Alter Content
Alter System
Disrupt an Organizations Ability to Make Informed Decisions
Malicious Modification of Key Information from Data Files
Insertion of Misinformation into Data Files
Destruction of Critical Data
Reformat Hard Drive
Delete Critical Database
Delete Critical Data
Conceal Malicious Behavior
Steganography
Encryption Tools
Event Log Tampering
Disrupt Network Performance and Reliability
Exploit Unpatched Systems
Launch Distributed Denial of Service Attack (DDOS)
Attack System with Known Exploit
Zero Day Attacks
Injecting Buffer Overflows
Take Over and/or Corrupt Computers
Install Virus using a USB Device
Install Virus using a CD/DVD
Install Virus using a Floppy Drive
Install Virus using Mobile Code
Install Virus through E-mail Attachments
Install Logic Bomb
Install Worm
Install Trojan Horse
Install Browser Hijacker
Install Backdoor
Install Dialer
Install Rootkit
Lock out Administrator Access
Lock out System Users
Create Rogue Accounts
Unauthorized User Activity Monitoring
Install Spyware
Install Sniffer
Install Keystroke Logger
Install Surveillance Software

Figure C.1: Insider Threat Decomposed Alteration Model

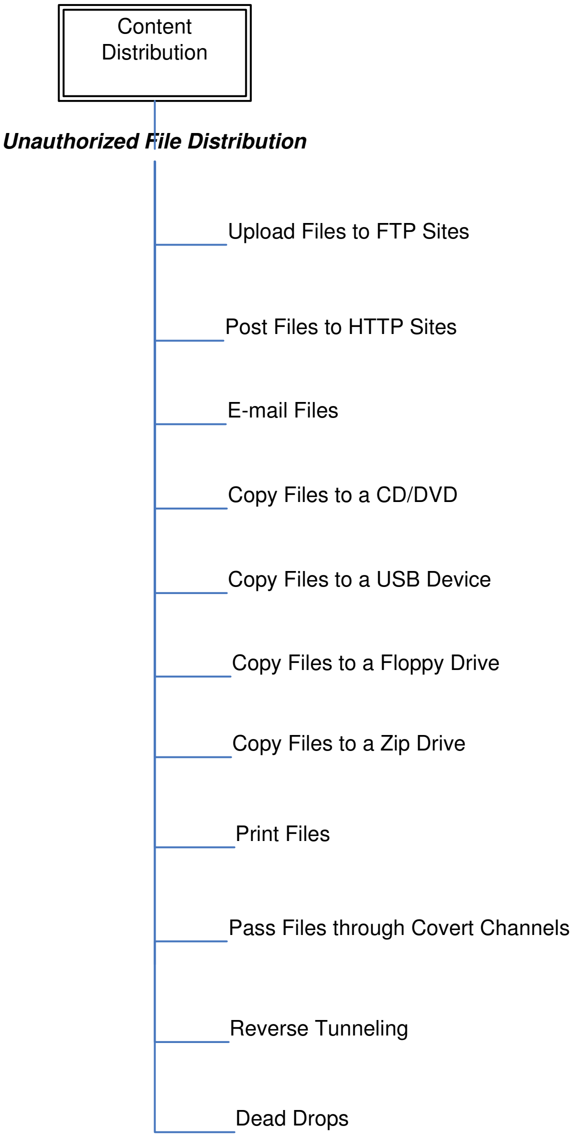

Content Distribution
Unauthorized File Distribution
Upload Files to FTP Sites
Post Files to HTTP Sites
E-mail Files
Copy Files to a CD/DVD
Copy Files to a USB Device
Copy Files to a Floppy Drive
Copy Files to a Zip Drive
Print Files
Pass Files through Covert Channels
Reverse Tunneling
Dead Drops

Figure C.2: Insider Threat Decomposed Distribution Model

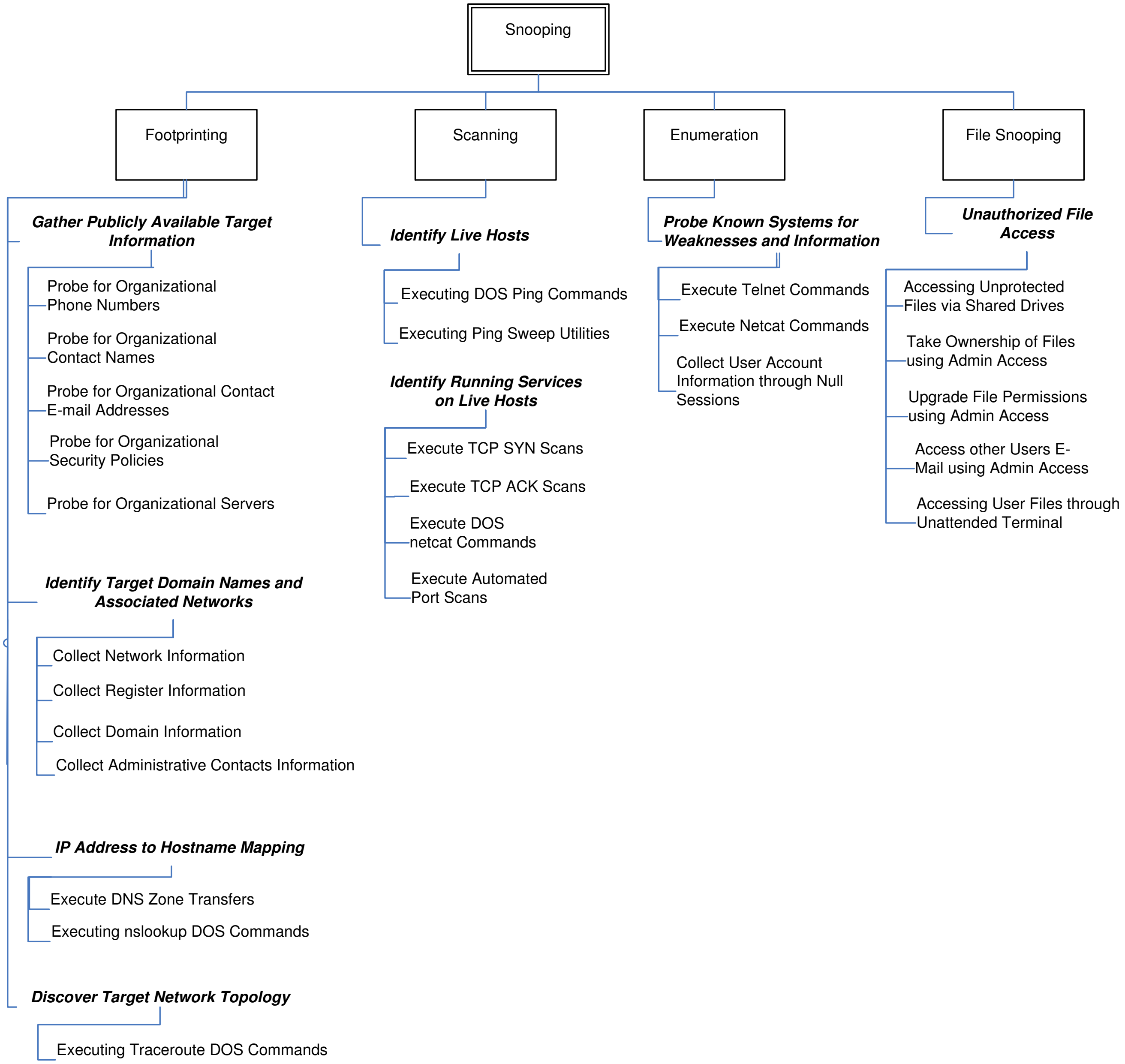

Snooping
Footprinting
Scanning
Enumeration
File Snooping
Gather Publicly Available Target Information
Probe for Organizational Phone Numbers
Probe for Organizational Contact Names
Probe for Organizational Contact E-mail Addresses
Probe for Organizational Security Policies
Probe for Organizational Servers
Identify Target Domain Names and Associated Networks
Collect Network Information
Collect Register Information
Collect Domain Information
Collect Administrative Contacts Information
IP Address to Hostname Mapping
Execute DNS Zone Transfers
Executing nslookup DOS Commands
Discover Target Network Topology
Executing Traceroute DOS Commands
Identify Live Hosts
Executing DOS Ping Commands
Executing Ping Sweep Utilities
Identify Running Services on Live Hosts
Execute TCP SYN Scans
Execute TCP ACK Scans
Execute DOS netcat Commands
Execute Automated Port Scans
Probe Known Systems for Weaknesses and Information
Execute Telnet Commands
Execute Netcat Commands
Collect User Account Information through Null Sessions
Unauthorized File Access
Accessing Unprotected Files via Shared Drives
Take Ownership of Files using Admin Access
Upgrade File Permissions using Admin Access
Access other Users E-Mail using Admin Access
Accessing User Files through Unattended Terminal

Figure C.3: Insider Threat Decomposed Snooping Model

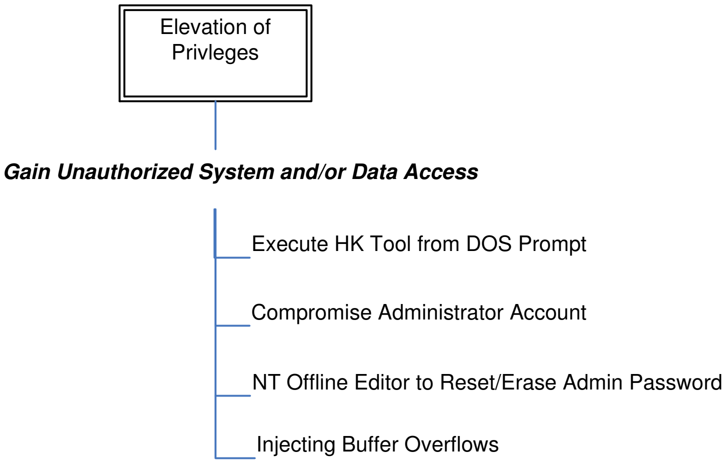

Elevation of Privleges
Gain Unauthorized System and/or Data Access
Execute HK Tool from DOS Prompt
Compromise Administrator Account
NT Offline Editor to Reset/Erase Admin Password
Injecting Buffer Overflows

Figure C.4: Insider Threat Decomposed Elevation Model

Bibliography

1. "CERT Overview Incident and Vulnerability Trends", March 2000.

2. Bishop, Matt. *Computer Security: Art and Science*. Addison-Wesley, Boston MA, 2003.

3. Brackney, Richard C. and Robert H. Anderson. *Proceedings of a 2004 Workshop: Understanding the Insider Threat*. RAND Corporation, Rockville, MD, March 2004.

4. Butts, J., R. Mills, and R. Baldwin. "Developing an Insider Threat Model Using Functional Decomposition". *Proceedings of the 2005 Mathematical Methods, Models, and Architecture for Computer Network Security workshop*, 412–417. St. Petersburg Russia, September 2005.

5. Center, CERT Coordination. "Secret Service and CERT Release Report Analyzing Acts of Insider Sabotage via Computer Systems in Critical Infrastructure Sectors". CERT Press Release, May 2005.

6. Chinchani, R., A. Iyer, H. Ngo, and S. Upadhyaya. "Towards a Theory of Insider Threat Assessment". *Proceedings of the 2005 International Conference on Dependable Systems and Networks*, 108–117. Yokohama Japan, June 2005.

7. Cole, Eric. *Insider Threat: Protecting the Enterprise from Sabatoge, Spying and Theft*. Syngress Publishing, Rockland, MA, 2006.

8. CSO Magazine, U.S. Secret Service and CERT Coordination Center. "2004 E-Crime Watch Survey". CSO Magazine, May 2005.

9. Dix, Alan, Janet Finlay, Gregory Abowd, and Russell Beale. *Human-Computer Interaction*. Prentice Hall, New York, NY, third edition, 2003.

10. DoD. *Information Assurance (IA) Implementation (8500.2)*. Technical report, Department of Defense, February 2003.

11. Feringa, A., A. Goguen, and G. Stoneburner. "Natational Institute for Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Technology Systems". In-house, 2002.

12. Finlay, P. N. *Introducting Decision Support Systems*. Blackwell Publishers, Oxford, MASS, 1994.

13. Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson. "2002 CSI/FBI Computer Crime and Security Survey". Computer Security Institute, March 2002.

14. Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson. "2003 CSI/FBI Computer Crime and Security Survey". Computer Security Institute, March 2003.

15. Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson. "2004 CSI/FBI Computer Crime and Security Survey". Computer Security Institute, May 2005.

16. Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson. "2005 CSI/FBI Computer Crime and Security Survey". Computer Security Institute, January 2006.

17. Haettenschwiler, P. "Neues anwenderfreundliches Konzept der Entscheidungsunterst". 189–208. 1999.

18. Irwin, Steven. "Former FAA engineer indicted in O'Hare code theft". http://archives.californiaaviation.org/airport/msg02974.html, October 1999.

19. Johnston, Roger G. "Adversarial Vulnerability Assessment". http://pearl1.lanl.gov/seals/.

20. Keeney, M., E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, and S. Rogers. "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors", May 2005. U.S. Secret Service and CERT Coordination Center/SEI.

21. Keeney, Michelle, Eileen Kowalski, Dawn Cappelli, and Andrew Moore. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*. Technical report, Secret Service National Threat Assessment Center and CERT Coordination Center, August 2004.

22. Krim, Jonathan and David A. Vise. "AOL Employee Charged in Theft Of Screen Names". http://www.washingtonpost.com/wp-dyn/articles/A860-2004Jun23.html, June 2004.

23. Magazine, CyberDefense. "Beware of Insider Threats to Your Security". http://www.viack.com/_download/200408_cdm.pdf, August 2004.

24. Maybury, M., P. Chase, B. Cheikes, D. Brackney, S. Matzner, T. Hetherington, B. Wood, C. Sibley, J. Marin, T. Longstaff, L. Spitzner, J. Haile, J. Copeland, and S. Lewandowski. "Analysis and Detection of Malicious Insiders", 2005. Submitted to 2005 International Conference on Intelligence Analysis, McLean VA.

25. Maybury, Mark and Penny Chase. "Insider Threat: Analysis and Detection of Malicious Insiders". Report, 2005.

26. Power, Daniel J. *Decision Support Systems: Concepts and Resources for Managers*. Quorumbooks, Westport, Connecticut, 2002.

27. Saleeba, David A. "Physical Security Vulnerability Risk Assessments". In-House, July 2004.

28. Sandhu, R. "The Schematic Protection Model: Its Definition and Analysis for Acyclic Attenuating Schemes". *Journal of the Association for Computing Machinery*, 35(2):404–432, April 1988.

29. Schneier, Bruce. "Attack Trees". Dr. Dobbs Journal, December 1999.

30. Schultz, E. "A Framework for Understanding and Predicting Insider Attacks". *Computer & Security*, 21(6):525–531, October 2002.

31. Shaw, Eric, Keven Ruby, and Jerrold Post. "The Insider Threat to Information Systems". 27–46. Security Awareness Bulletin, June 2002.

32. Spitzner, Lance. "Honeypots Catching the Insider Threats". *19th Annual Computer Security Applications Conference*, 170–181. IEEE Computer Society, 2003. ISBN 0-7695-2041-3.

33. Spitzner, Lance. "Honeypots: The Other Honeypot". http://www.securityfocus.com/infocus/1713, July 2003.

34. von Winterfeldt, Detlof and Ward Edwards. *Decision Analysis and Behavioral Research*. Cambridge University Press, Cambridge, United Kingdom, 1986.

35. Wise, David. *Nightmover: How Aldrich Ames Sold the CIA to the KGB*. Harpercollins, New York, NY, 1995.

36. Wood, B. "An Insider Threat Model for Adversary Simulation". SRI International Cyber Defense Research Center, Albuquerque NM, July 2000.

37. Wood, Bradley J. "An Insider Model for Adversary Simulation". http://www.cert.org/present/cert-overview-trends/module-2.pdf, 2002. Appendix B.

38. Yee, Jason. *Efficient Generation of Social Network Analysis Data From Computer-Mediated Communication Logs*. Master's thesis, Graduate School of Engineering, Air Force Institute of Technology (AETC), Wright-Patterson AFB OH, March 2005. AFIT/EN/ENG/GCS-05M.

Vita

Marine Corps Gunnery Sergeant William H. King graduated from Kahlotus High School in Kahlotus, Washington. In March 1994, he enlisted in the United States Marine Corps. Upon completion of recruit training in San Diego, CA he attended Marine Combat Training (MCT). Upon completion of MCT, he attended military occupational specialty (MOS) training.

Following MOS training in October 1994, Gunnery Sergeant King was assigned to his first duty station: 1st Battalion, 7th Marines, 1st Marine Division in Twentynine Palms, CA. During his tenure with 1st Battalion, 7th Marines some of the billets he held included battalion legal and administration chief. While serving with 1st Battalion, 7th Marines he completed two unit deployment rotations to Okinawa, Japan.

In 1998, he attended military occupational training at the Communications and Electronics School in Twentynine Palms and was subsequently assigned to the Defense Finance and Accounting Service Center (DFAS) in Kansas City, MO.

In May 2001, Gunnery Sergeant King was transferred to the Marine Corps Recruit Depot, San Diego, CA to serve as the Recruit Depot's Computer Network Manager.

Gunnery Sergeant King graduated cum laude from National University in January 2004. He is scheduled to graduate from AFIT in June 2006 with a Master of Science Degree with a concentration in Information Assurance. After graduation, Gunnery Sergeant King has been selected for a follow on assignment to the Third Marine Expeditionary Force in Okinawa, Japan to serve as the Assistant Chief of Staff G-6, Information Assurance Officer.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 13-06-2006	**2. REPORT TYPE** **Master's Thesis**	**3. DATES COVERED** *(From – To)* May 2005-June 2006

4. TITLE AND SUBTITLE Development of an Malicious Insider Composite Vulnerability Assessment Methodology	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) King, William H., Gunnery Sergeant, USMC	**5d. PROJECT NUMBER** If funded, enter ENR #
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GIA/ENG/06-06
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Trusted employees pose a major threat to information systems. Despite advances in prevention, detection, and response techniques, the number of malicious insider incidents and their associated costs have yet to decline. There are very few vulnerability and impact models capable of providing information owners with the ability to comprehensively assess the effectiveness an organization's malicious insider mitigation strategies.
This research uses a multi-dimensional approach: content analysis, attack tree framework, and an intent driven taxonomy model are used to develop a malicious insider Decision Support System (DSS) tool.
The DSS tool's utility and applicability is demonstrated using a notional example. This research gives information owners data to more appropriately allocate scarce security resources.

15. SUBJECT TERMS
Insider threat, security model, vulnerability assessment, information security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** **Robert F. Mills, PhD (ENG)**
REPORT **U**	**ABSTRACT** **U**	**c. THIS PAGE** **U**	**UU**	105	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565 ext 4527; email: robert.mills@afit.edu